Uniform Embedding for Efficient JPEG Steganography

Linjie Guo, *Student Member, IEEE*, Jiangqun Ni, *Member, IEEE*, and Yun Qing Shi, *Fellow, IEEE*

***Abstract*— Steganography is the science and art of covert communication, which aims to hide the secret messages into a cover medium while achieving the least possible statistical detectability. To this end, the framework of minimal distortion embedding is widely adopted in the development of the steganographic system, in which a well designed distortion function is of vital importance. In this paper, a class of new distortion functions known as uniform embedding distortion function (UED) is presented for both side-informed and non side-informed secure JPEG steganography. By incorporating the syndrome trellis coding, the best codeword with minimal distortion for a given message is determined with UED, which, instead of random modification, tries to spread the embedding modification uniformly to quantized discrete cosine transform (DCT) coefficients of all possible magnitudes. In this way, less statistical detectability is achieved, owing to the reduction of the average changes of the first- and second-order statistics for DCT coefficients as a whole. The effectiveness of the proposed scheme is verified with evidence obtained from exhaustive experiments using popular steganalyzers with various feature sets on the BOSSbase database. Compared with prior arts, the proposed scheme gains favorable performance in terms of secure embedding capacity against steganalysis.**

***Index Terms*— JPEG steganography, minimal-distortion embedding, uniform embedding, distortion function design.**

I. Introduction

STEGANOGRAPHY is the science and art of covert communication where the sender embeds secret message into an original image (cover) with a shared key to generate a stego image. To conceal the very existence of communication, the stego image has to be statistically undetectable from its cover counterpart [1]. Therefore, the two conflicting objectives, i.e., undetectability and embedding payload, should be carefully considered when devising a steganographic scheme. Denote $\mathbf{x} \in \mathrm{R}^n$ and $\mathbf{y} \in \mathrm{R}^n$ as the cover and stego images, respectively. We then define the cost (or distortion) function of making an embedding change at i-th element of $\mathbf{x}$ from x_i to y_i as $\rho_i(x_i, y_i)$, where $0 \leq \rho_i < \infty$. Under the additive distortion model, the total impact caused by the embedding can be expressed as the sum of embedding cost over all elements, i.e., $D(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} \rho_i(x_i, y_i)$. In practice, the problem of designing a secure steganographic scheme can be formulated as the minimal distortion embedding, i.e., to minimize the total embedding distortion D for a given payload. With properly designed ρ_i, the total statistical artifacts caused by the embedding are minimized and the resulting stego objects can be made less detectable.

As JPEG is the most widely used format for digital image storage and transmission, JPEG steganography has become the domain of extensive research. It has witnessed the development of a lot of schemes for JPEG steganography over the last decade, such as F5 [2], nsF5 [3], MME [4] and some recently emerged adaptive ones [5]–[7]. All of these schemes can be described with a unified framework — the minimal distortion embedding framework, which consists of the coding unit and the distortion function. In the F5, the embedding impact is treated equally for each coefficient. As a result, minimizing the total distortion for a given payload corresponds to the effort to minimize the number of coefficients to be modified, or maximize the embedding efficiency, i.e., the number of message bits embedded per embedding change. The security performance of F5 was improved by increasing its embedding efficiency through matrix encoding, which can be viewed as a special case of the minimal distortion embedding framework with the embedding cost being identical for each coefficient. In [3], the wet paper code (WPC) is incorporated in nsF5, improved version of F5, to tackle the issue of shrinkage with F5, resulting in significant improvement in coding efficiency compared to the Hamming code used in F5. In the MME, for JPEG steganography, the advantage of the side-information of the original uncompressed image is taken to construct the distortion function, furthermore, only those coefficients with less distortion are selected to be modified, and more coefficients may be modified compared with the matrix coding. Later, Sachnev *et al.* proposed in [5] another efficient JPEG steganographic scheme, denoted as BCHopt, based on heuristic optimization and fast BCH syndrome coding. Compared with the MME, the BCHopt takes into account not only the rounding error but also the quantization step in the construction of distortion function, thus leading to significant improvement in security performance against steganalysis. The

Manuscript received August 18, 2013; revised January 6, 2014 and February 20, 2014; accepted March 4, 2014. Date of publication March 20, 2014; date of current version April 10, 2014. This work was supported in part by the National Natural Science Foundation of China under Grants 61379156 and 60970145, in part by the National Research Foundation for the Doctoral Program of Higher Education of China under Grant 20120171110037, and in part by the Key Program of Natural Science Foundation of Guangdong under Grant S2012020011114. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Patrick Bas.

L. Guo and J. Ni are with the School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510006, China (e-mail: g.linjie@gmail.com; issjqni@mail.sysu.edu.cn).

Y. Q. Shi is with the Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ 07102 USA (e-mail: shi@njit.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2014.2312817

performance gain of both MME and BCHopt stems largely from the original BMP image as precover, which is, however, not always available in practice.

In [1], Filler *et al.* proposed to use syndrome trellis coding (STC) as a practical approach for the implementation of minimal distortion embedding framework. They have shown that, under the additive distortion model, the STC can achieve asymptotically the theoretical bound of embedding efficiency for a user-defined distortion function. With the emergence of this efficient coding method, it is increasingly recognized in the steganographic community that further substantial increase in secure payload for steganography is more likely achieved by properly designing the distortion function rather than improving the coding scheme itself.

In [6], Filler and Fridrich proposed a rich parametric model for the embedding cost at a specific coefficient by taking into account both the coefficient itself and its neighborhoods. By incorporating the STC, they optimized the constructed cost model with respect to the popular steganalysis feature set CC-PEV-548D [8]. The experimental results showed that the proposed distortion function, a.k.a. Model Optimized Distortion (MOD), can significantly improve the secure payload in DCT domain. However, as reported in a later paper by Kodovský *et al.* [9], the security performance of MOD can be drastically degraded as the distortion is optimized w.r.t. an incomplete feature space. By enlarging the corresponding parts of CC-PEV model, the MOD can be reliably detected by the IBC-EM feature set [9], and even becomes less secure than the heuristically designed nsF5.

More recently, Holub and Fridrich proposed a universal distortion design called UNIWARD [10], in which the distortion functions for spatial (S-UNI), JPEG (J-UNI) and side-informed JPEG (SI-UNI) domain are derived from the wavelet domain. Unlike the conventional JPEG steganographic schemes which only embed the secret message into non-zero AC coefficients, the UNIWARD uses all DCT coefficients (DCs, zero and non-zero ACs) as possible cover elements for steganography, thus achieves so far the best security performance.

Corresponding to the development of JPEG steganography, substantial progress has also been made recently in JPEG steganalysis. In [11], Kodovský and Fridrich suggested using a rich model with a large feature set of up to 22,510-D for steganalysis. By using the ensemble classifier [12], the rich model based steganalysis can detect most existing JPEG steganographic algorithms with a high accuracy. Consequently, the secure payload of JPEG steganography is decreased substantially, which poses new challenges on modern JPEG steganography. Therefore, there is an increasing need to develop more secure JPEG steganography algorithms.

In general, a good JPEG steganographic scheme involves two aspects, i.e., an efficient steganographic coding unit and an effective distortion function which is correlated with the statistical detectability. In this paper, we focus on the design of a new additive distortion function for JPEG steganography. By following the concept in spirit of "spread spectrum communication", the proposed distortion function is designed so as to guide the stego system to uniformly "spread" the embedding modification to the quantized DCT coefficients of all possible magnitudes. This results in possible minimal artifacts of first- and second-order statistics for DCT coefficients as a whole. It is noted that, for non side-informed JPEG steganography, our proposed distortion function is derived directly from the quantized block DCT coefficients without any pre-model training. An efficient JPEG steganographic scheme is then developed by incorporating the new distortion function in the STC framework, which works quite well against the popular steganalyzers with various feature sets, e.g., CC-PEV-548D [8], IBC-EM-882D [9], MP-486D [13], and the recently emerged state-of-the-art feature set, CC-JRM-22,510D [11]. In addition, if available, the original BMP image can be used as precover (side information) to further improve the security performance of our method.

As an extension of our previous work in [14], this paper includes several new contributions: 1) the detailed analysis why the proposed UED function can lead to less average changes of second-order statistics besides the first-order ones; 2) the analysis of the allowable modification (embedding) rate of DCT coefficients with different magnitude from the perspective of natural image model; 3) the new scheme for side-informed JPEG steganography; and 4) implementation of all the experiments on the new BOSSbase [15] image database, which is widely considered as a more appropriate benchmark to evaluate the performance of the steganographic and steganalytic schemes.

The remainder of this paper is organized as follows. In Section II, the adaptive steganographic framework for minimal distortion embedding is briefly reviewed. The proposed distortion function and the new JPEG steganographic scheme are presented in Section III and IV, respectively, which are followed by the experimental results and analysis in Section V. Finally the concluding remarks are summarized in Section VI.

II. Practical Minimal Distortion Embedding Framework

In steganography, the transmitter uses seemingly innocent media, e.g., digital images, to hide her messages and communicate with the receiver. In this way, it is hard to distinguish the stego media from the cover one, and thus covert communication can be achieved. In the literature, the message is generally hidden (embedded) in the cover image by slightly modifying some individual elements of cover, such as LSBs of pixels and quantized DCT coefficients. The problem of minimizing the embedding impact for single-letter distortion is well formulated in [1]. Let the binary vector $\mathbf{x}_b = [x_{b1}, x_{b2}, \ldots, x_{bn}]$, $\mathbf{y}_b = [y_{b1}, y_{b2}, \ldots, y_{bn}] \in \{0, 1\}^n$ and $\mathbf{m} = [m_1, m_2, \ldots, m_k] \in \{0, 1\}^k$ be the LSB vector of cover $\mathbf{x}$, LSB vector of stego $\mathbf{y}$ and message, respectively, we have the additive cost function as

$$D(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} \rho_i(\mathbf{x}, y_i), \tag{1}$$

where $\rho_i(\mathbf{x}, y_i)$ denotes the cost of changing the i-th cover element from x_i to y_i. With the syndrome coding, the minimal

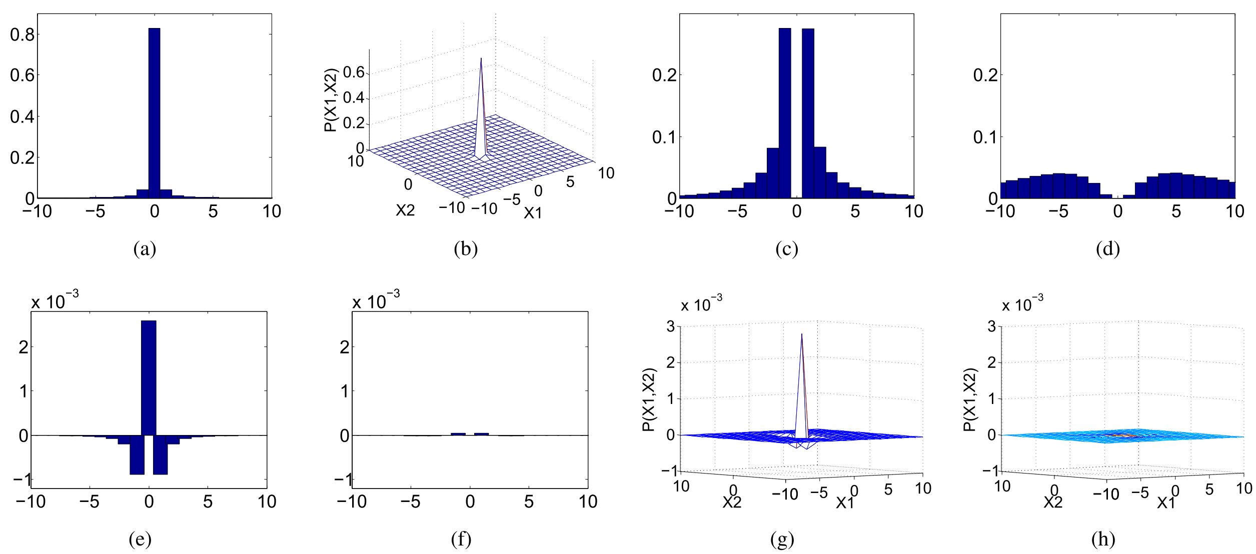


Fig. 1. Comparison of statistics changes between nsF5 and the UED. (a) and (b) are the DCT coefficients histogram and the co-occurrence matrix of neighboring DCT coefficients for cover images. (c) and (d) are the histograms for the modified coefficients with nsF5 and the proposed scheme at 0.2 bpac, respectively. (e) and (g) are changes in statistics of (a) and (b) with nsF5. (f) and (h) are changes in statistics of (a) and (b) with the proposed scheme.

distortion embedding framework is formulated as

$$\begin{aligned} Emb\,(\mathbf{x}, \mathbf{m}) &= \arg\min_{\mathbf{y}_b \in C(\mathbf{m})} D\,(\mathbf{x}, \mathbf{y}) \\ \text{and } H\mathbf{y}_b &= \mathbf{m}, \end{aligned} \tag{2}$$

where H is parity-check matrix of the code C and $C\,(\mathbf{m})$ is the coset corresponding to syndrome $\mathbf{m}$.

In the minimal-distortion embedding framework, most existing coding methods including Hamming code, BCH code and STC can be adopted. For practical design of steganography, the performance of coding method can be well evaluated using the metric of **coding loss** defined as the relative decrease in payload due to practical coding [1]:

$$l(D_\varepsilon) = \frac{m_{\text{MAX}} - m}{m_{\text{MAX}}}, \tag{3}$$

where m is the payload embedded by a given algorithm and m_{MAX} is the maximal payload embeddable with a distortion not exceeding D_ε. Under this context, the Syndrome-Trellis Codes (STCs) [1] achieved an extremely low coding loss with $l = 7\% - 14\%$ depending on the parameter setting and thus is adopted in the construction of our proposed JPEG steganographic scheme.

As for the distortion function, instead of training it against any specific feature set, we attempt to design a "universal" one to make the possible minimal artifacts of first- and second-order statistics, which constitute the primitive elements of almost all feature sets for JPEG steganalysis.

III. Proposed Distortion Function

A. Motivation Behind Uniform Embedding Strategy

To detect JPEG steganography, the statistics of quantized DCT coefficients are often exploited to construct feature set for steganalyzers. In practice, the histogram and the co-occurrence matrix of the block DCT coefficients are widely used in steganalysis. While the former relates to the first-order statistics, and the latter corresponds to the second-order ones, which can capture the correlations among the DCT coefficients.

Once a secret message (payload) is embedded into a JPEG image, the statistics of the DCT coefficients will be modified to some extent, which leaves trace for steganalysis. The impacts of data embedding on the statistics of DCT coefficients are well illustrated with nsF5 [3] as shown in Fig. 1. To be more specific, we randomly select 2,000 images from BOSSbase [15] and JPEG compress them with QF $=$ 75. The average changes of statistics after steganography are then reported in Fig. 1. Fig. 1(a) shows the global histogram h of DCT coefficients X, and Fig. 1(b) corresponds to the co-occurrence matrix $P\,(X_1, X_2)$ of coefficient X_1 and its neighboring one X_2 with offset $d = (0, 1)$. For a given payload of 0.2 bpac, Fig. 1(c) shows the histogram of the DCT coefficients being selected to be modified by the nsF5 scheme, whereas Fig. 1(e) and (g) report the changes of h and $P\,(X_1, X_2)$ after nsF5 embedding, respectively. As shown, most of the modifications of DCT coefficient are observed around bin zero.

To gain insights on the artifacts we observe in Fig. 1, we now analyze how nsF5 works. For a given payload α, nsF5 embedding simulator [3] first calculates the theoretical bound of the embedding efficiency, and obtain the number n of the coefficients to be modified. Then, it randomly selects n nonzero AC coefficients and decreases their absolute value by 1. We use $p\,(x)$ and $p_{\text{nz}}\,(x)$ to denote the empirical probability density function (PDF) of the AC and nonzero AC coefficients, respectively. There are $n \cdot p_{\text{nz}}(x)$ AC coefficients at bin x that needs to be modified. Therefore, we can express the change of PDF due to message embedding as

$$\Delta p(x) = \begin{cases} n \cdot [p_{\text{se1}}(x-1) + p_{\text{se1}}(x+1)]/N & \text{if } x = 0 \\ n \cdot [p_{\text{se1}}(x+\text{sgn}(x)) - p_{\text{se1}}(x)]/N & \text{if } x \neq 0, \end{cases} \tag{4}$$

where $p_{\text{sel}}(x) = p_{\text{nz}}(x)$ is the probability that coefficient x is selected and N denotes the total number of all the block DCT coefficients.

Considering the fact that the block DCT coefficients are approximately Laplacian distributed and the random selection nature of nsF5, the coefficients to be modified are most likely those with small magnitude. As a result, most of the coefficient modifications due to this embedding strategy occur around bin zero. As observed in Fig. 1(c), most of the coefficients to be modified are located within bins of absolute value 2. According to (4), the changes of statistics in bin 0 and ± 1 arising from random embedding are significantly larger than the ones in other bins as shown in Fig. 1(e).

By exploiting the mentioned distribution artifacts of DCT coefficients with small magnitude ($|X| \leq T$), even when the threshold $T = 2$, most existing JPEG steganalyzers, e.g., CC-PEV-548D [8] can detect JPEG steganography with high accuracy. For JPEG steganography, although the number of modified coefficients would be reduced if a more efficient coding strategy is adopted, the distribution of the modified coefficients, however, would remain similar after embedding. As a result, the substantial statistical artifacts of small DCT coefficients can still be made use of to detect stego JPEG images, especially when relative large data payload is required. To avoid the sudden change of statistics in small DCT coefficients, uniform embedding (UE) as formulated in (5) is more preferable rather than the random embedding strategy.

$$p_{\text{sel}}(x+\text{sgn}(x)) \cong p_{\text{sel}}(x), \quad x \in \{-1024, \ldots, -1, 1, \ldots, 1024\}. \tag{5}$$

The uniform embedding strategy tries to "spread" the embedding modifications to coefficients of all possible magnitudes so as to minimize the statistics change in each bin, i.e.,

$$\Delta p(x+\text{sgn}(x)) \cong \Delta p(x), x \in \{-1024, \ldots, -1, 1, \ldots, 1024\}. \tag{6}$$

To embed a given message M, let ΔM be the total modifications, and RN and UN be the bin numbers involved in random and uniform embedding, respectively. The "spread magnitude" nature of uniform embedding makes $UN \gg RN$, therefore the average modification per bin ($\Delta M \big/ UN$) for uniform embedding is much less than one ($\Delta M \big/ RN$) for random embedding. Note that, unlike OutGuess [16], our scheme seeks to minimize the change of the first-order statistics as well as the higher order ones. Take the $P(X_1, X_2)$ in Fig. 1(b) for example, where a 21×21 co-occurrence matrix (i.e., $|X_i| \leq 10, i = 1, 2$) averaged over 2,000 JPEG compressed images ($QF = 75$) is illustrated. The uniform embedding approach allows the modifications spreading over all quantized coefficients of different magnitudes, thus minimizing the change of each entry of $P(X_1, X_2)$ as shown in Fig. 1(h). In addition, the proposed scheme neither modifies the zero-coefficients nor creates new zero-coefficients.

In practice, the uniform embedding strategy can be implemented using STC [1]. To embed a given message, the STC provides multiple codewords, among which, a distortion function is then incorporated to choose the one with the least distortion. To be able to accomplish the uniform embedding, the involved distortion function should be designed so that the coefficients of different magnitude are selected with equal priority. In the following, we refer to such function as uniform embedding distortion function (UED). Let x denote the DCT coefficient, which is Laplacian distributed as shown in Fig. 2 (c.f. curve marked with 'a'). The distortion function used in UED should have the form of $\rho(x) = 1 \big/ |x|$, i.e., the selection probability of a coefficient x is monotonically increased with its magnitude $|x|$ as shown by the curve 'b' in Fig. 2. Curve 'c' in Fig. 2 shows the approximately uniform distribution of selected DCT coefficients when the UED is applied, which also corresponds to the less statistical detectability.

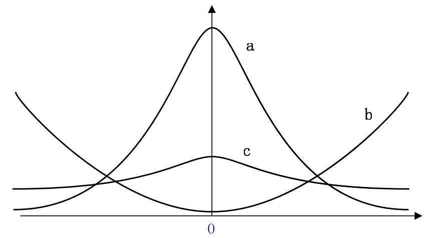


Fig. 2. Schematic illustration of the uniform embedding strategy. Curve 'a' is the distribution of DCT coefficients. Curve 'b' is the selection probability of each coefficient with UED. Curve 'c' is the distribution of the selected coefficients.

B. Model of Natural Image

It is obvious that the DCT coefficients with large amplitude tend to be modified more heavily than previous approaches, such as nsF5, when the strategy of uniform embedding is adopted. We then proceed to investigate the allowable modification (embedding) rate of DCT coefficients with different magnitude from the perspective of image model. The existing steganalysis analyzers for JPEG image generally take advantage of natural image model in terms of first- and second-order statistics of quantized DCT coefficients for steganalysis. If the distribution of DCT coefficients can be exactly characterized by some kind of image models, then any slight modification of the cover image will be reliably detected. Fortunately, the distributions of the DCT coefficients for natural images depend heavily on the image contents and vary from one to another. In other words, the statistics of natural images indeed exhibit, to some extent, deviation away from their models of any kinds, which are what the potentials of natural images left for steganography. To justify the deviation of natural images in terms of first- and second-order statistics, we again randomly selected 2,000 JPEG images from the image database BOSSbase [15]. The histogram of DCT coefficients $p(x)$ of each image is first calculated. And the mean value $\mu(x)$ and standard deviation $\sigma(x)$ of $p(x)$ are then obtained, respectively, as shown in Fig. 3(a) and (b). The existence of $\sigma(x)$ indicates the dispersion of natural images in first-order statistics, which is more appropriate to be measured using the normalized *coefficient of variation* (CV) [17] defined as the ratio of the standard deviation to the mean:

$$Cv(x) = \frac{\sigma(x)}{\mu(x)}. \tag{7}$$

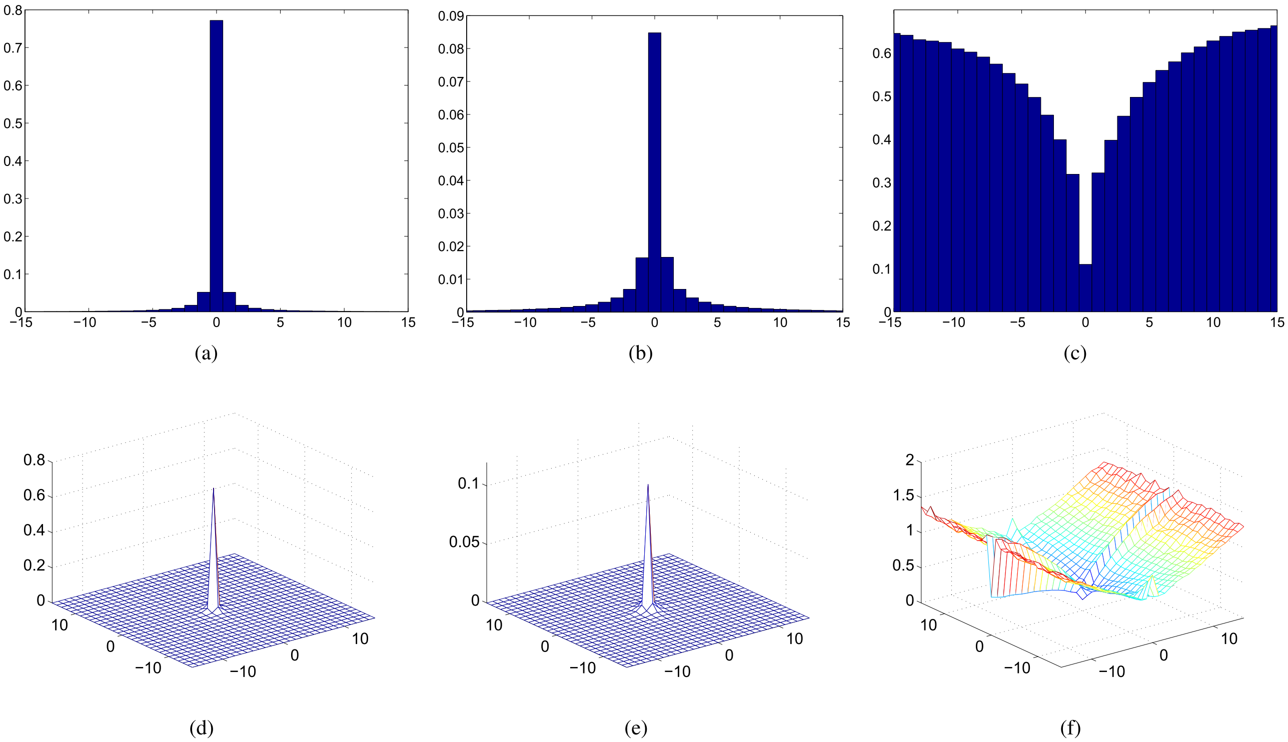


Fig. 3. (a)–(c) and (d)–(f) are the mean, standard deviation and CV of $p(x)$ and $P(X_1, X_2)$ over 2,000 JPEG image, respectively.

As is shown in Fig. 3(c), $Cv(x)$ increases with $|x|$, which implies that, for natural images, the histogram of quantized DCT coefficients $p(x)$ tends to deviate heavily when the magnitude of coefficients (i.e., $|x|$) increase. Therefore, if the relative modification rate of each x is proportional to its CV so as to make the uniform modification across all x, the statistical impact in first-order statistics could be minimized.

The similar effect is also observed with second-order statistics of natural images. Let $P(X_1, X_2)$ denote the co-occurrence matrix with offset $d = (0, 1)$. Fig. 3(d)–(f) show the mean $\mu(X_1, X_2)$, standard deviation $\sigma(X_1, X_2)$ and normalized *coefficient of variation* $Cv(X_1, X_2)$ of $P(X_1, X_2)$ over 2,000 JPEG images with $QF = 75$, respectively. Obviously, $Cv(X_1, X_2)$ also increases with the increase of $|X_1| + |X_2|$. In other words, it is more difficult to model the second-order statistics of DCT coefficients when $|X_1| + |X_2|$ gets larger. Therefore, the statistical impact of modifying a DCT coefficient x depends on its own magnitude $|x|$ as much as on the magnitudes of its neighboring coefficients.

C. Distortion Function for the Uniform Embedding Strategy

1) Single Coefficient Based Uniform Embedding Distortion: Let c_{ij} denote the DCT coefficient at (i, j), the distortion function of form $1/|c_{ij}|$ is well explained with the concept of uniform embedding. It is intuitive to define the single coefficient based uniform embedding distortion function (SC-UED) as below:

$$\rho_{ij}^{\mathrm{SC}} = |c_{ij}|^{-1}. \tag{8}$$

With SC-UED and the STC framework, for 2,000 JPEG images with $QF = 75$, the statistics changes after steganography of 0.2 bpac are also shown in Fig. 1. It is observed that the selected coefficients are much more uniformly distributed [Fig. 1(d)] than the ones with random selection of nsF5 [Fig. 1(c)]. Compared to Fig. 1(e) and (g) of nsF5, the uniform embedding has a quite uniform distribution and much less average changes in first- and second-order statistics, e.g., the global histogram and co-occurrence matrix with offset $d = (0, 1)$, as shown in Fig. 1(f) and (h). No notable sudden changes in statistics are observed, especially in the region of small coefficients, say, $[-2, 2]$.

2) Joint Coefficients Based Uniform Embedding Distortion: The SC-UED is employed to effectively relieve the sudden statistical changes, especially for the first-order statistics, due to random embedding. To survive the attacks of existing and emerging steganalysis tools [8], [11], [13], a better distortion function should be devised to allow a more uniform change of both first- and second-order statistics. For JPEG steganalysis, the second-order statistics of the DCT coefficients are generally characterized with co-occurrence matrix, i.e., $P(X_1, X_2)$, where X_1 and X_2 are the quantized DCT coefficient and its neighboring one with offset d, respectively. Following the concept of SC-UED, and noting the fact that the quantized DCT coefficient pair (X_1, X_2) is generally 2-D Laplacian distributed, the (X_1, X_2) with larger magnitude should be modified with priority during embedding. Therefore, to design the practical UED for a quantized DCT coefficient, besides the magnitude of the DCT coefficient itself, the ones of its intra- and inter-block neighborhood coefficients which are assumed to have the strongest magnitude correlation with the coefficient under consideration, should be taken into account. The developed distortion function is known as the joint coefficients based uniform embedding distortion (JC-UED) and

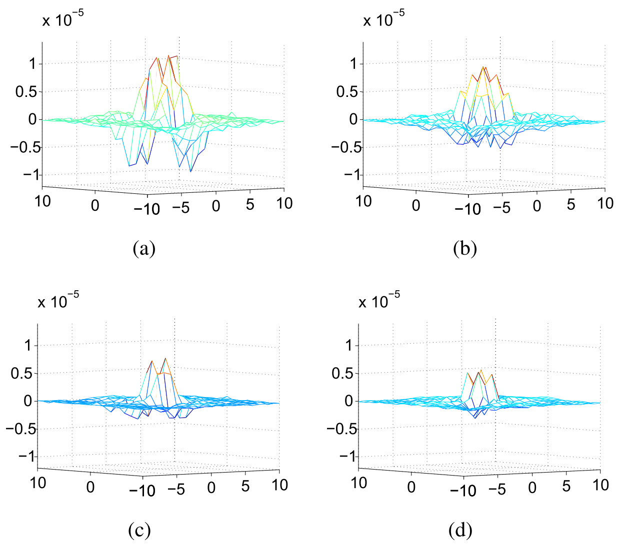


Fig. 4. (a)–(b) are changes of co-occurrence matrix with offset $d = (0, 1)$ and $d = (0, 8)$ of SC-UED, respectively. (c)–(d) are same statistics changes of JC-UED. The payloads are both 0.2 bpac.

described in (9)

$$\rho_{ij}^{\mathrm{JC}} = \sum_{d_{\mathrm{ia}} \in N_{\mathrm{ia}}} \left(|c_{ij}| + |d_{\mathrm{ia}}| + \alpha_{\mathrm{ia}}\right)^{-1} + \sum_{d_{\mathrm{ir}} \in N_{\mathrm{ir}}} \left(|c_{ij}| + |d_{\mathrm{ir}}| + \alpha_{\mathrm{ir}}\right)^{-1}, \tag{9}$$

where $N_{\mathrm{ia}} = \{c_{i+1,j}, c_{i-1,j}, c_{i,j+1}, c_{i,j-1}\}$ and $N_{\mathrm{ir}} = \{c_{i+8,j}, c_{i-8,j}, c_{i,j+8}, c_{i,j-8}\}$ are intra- and inter-block neighborhoods of coefficient c_{ij}, respectively. When the considered coefficient c_{ij} is located in the image boundary, the nonexistent coefficients are removed from (9) accordingly. α_{ia} and α_{ir} are adjustment parameters and determined experimentally as 1.3 and 1, respectively, as in [14]. The way how these two parameters are experimentally determined is as below:

1) Randomly select 2,000 images from the image database described in [14], and set a fixed payload (e.g. 0.3 bpac);
2) Estimate the error probability with the CC-JRM features utilizing the ensemble classifier on the grid: $\mathcal{A}_{\mathrm{ia}} \times \mathcal{A}_{\mathrm{ir}}$, where $\mathcal{A}_{\mathrm{ia}} = \{0, 0.1, \ldots, 1.9, 2\}$ and $\mathcal{A}_{\mathrm{ir}} = \{0, 0.1, \ldots, 1.9, 2\}$;
3) Select the best parameter pair with the minimum error probability as α_{ia} and α_{ir}.

According to our experiments, the variations of the estimated parameters α_{ia} and α_{ir} are little for different image database.

Fig. 4 shows the changes of second-order statistics with different distortion functions, where Fig. 4(c) and (d) are changes of co-occurrence matrix of offset $d = (0, 1)$ and $d = (0, 8)$ with JC-UED, compared with ones of the same offset with SC-UED in Fig. 4(a) and (b), suggesting that the JC-UED can well improve the sudden changes of the second-order statistics changes. Or, in other words, the JC-UED makes both the first- and second-order statistics change more uniformly.

3) Side-Informed Uniform Embedding Distortion: In general, the original BMP image as side-information can help to design efficient JPEG steganographic scheme [4], [5], [7]. Although the original BMP image is not necessary in the construction of UED, it is expected that the performance of the proposed scheme can be greatly improved by taking into account the side-information when it is available. The developed distortion function is referred to as side-informed uniform embedding distortion (SI-UED), which should satisfy both the requirements of uniform embedding and minimizing the absolute distortion, i.e., the additional rounding error as well.

With the original BMP image, the rounding error R due to JPEG compression and the embedding error R' due to data embedding are readily obtained. Thus we have the resulting additional rounding error $E = |R' - R|$, which is incorporated in the construction of SI-UED and has to be minimized. As a result, the SI-UED is defined as

$$\rho_{ij}^{\mathrm{SI}} = e_{ij} \cdot \Big[\sum_{d_{\mathrm{ia}} \in N_{\mathrm{ia}}} (|c_{ij}| + |d_{\mathrm{ia}}| + \alpha_{\mathrm{ia}})^{-1} + \sum_{d_{\mathrm{ir}} \in N_{\mathrm{ir}}} (|c_{ij}| + |d_{\mathrm{ir}}| + \alpha_{\mathrm{ir}})^{-1} \Big], \tag{10}$$

where e_{ij} is the additional rounding error for c_{ij}, α_{ia} and α_{ir} are adjustment parameters determined experimentally as 0.2 (obtained using the similar procedure described in the previous subsection), other parameters are similarly defined as the ones in (9).

The MME [4] is the first side-informed JPEG steganographic scheme that tried to improve its security performance by minimizing the additional rounding error. According to [4], modifying the coefficients with rounding error closer to 0.5 leads to less additional rounding errors. The BCH [5] and EBS [7] are also side-informed schemes that utilizing the rounding error. The feasibility of the SI-UED is illustrated in Fig. 5, where the average distributions of rounding error, i.e., frequency vs. rounding error [Fig. 5(a), (c), (e), and (g)] and the average changes in global histogram [Fig. 5(b), (d), (f), and (h)] for MME, BCH, EBS and SI-UED over 2,000 images randomly selected from the BOSSbase with a payload of 0.3 bpac are included. For fair comparison, all the four schemes are STC coded. It is observed that all the four schemes tend to modify more coefficients with rounding error close to 0.5, whereas less coefficients with rounding error close to 0. Compared with Fig. 5(a) and (c), the SI-UED modifies a little bit more coefficients with rounding error close to 0. This is because the SI-UED has to take the uniform embedding strategy into account at the same time, which consequently leads to much less statistical changes as shown in Fig. 5(h). Fig. 5(b), (d), (f), and (h) are average changes in global histogram caused by the MME, BCH, EBS and SI-UED, respectively. Again, compared with SI-UED [Fig. 5(h)], it is noted that the other schemes give rise to a much more sudden changes in the bins around zero coefficient as shown in Fig. 5(b), (d), and (f), as nsF5 does, especially the MME.

IV. Proposed JPEG Steganographic Scheme

The objective of minimal distortion embedding framework is to improve the security performance of steganography.

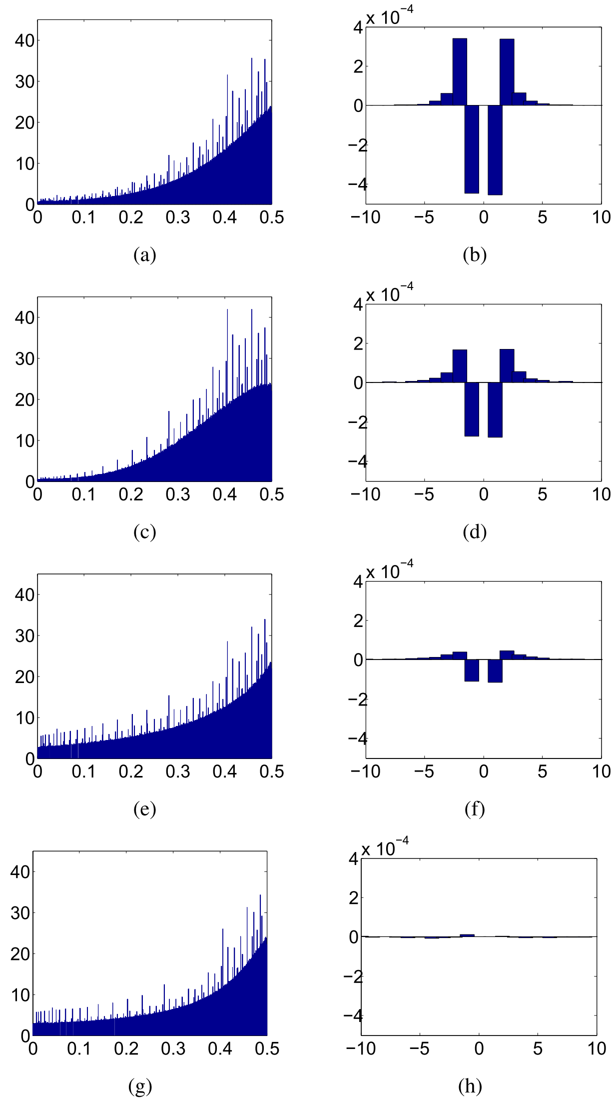


Fig. 5. (a), (c), (e) and (g) are the average distribution of the rounding errors of the modified coefficients over 2,000 images for MME, BCH, EBS and SI-UED, respectively; (b), (d), (f) and (h) are average changes in global histogram over 2,000 images for MME, BCH, EBS and SI-UED, respectively. All of the four schemes are STC coded with a payload of 0.3 bpac.

To this end, syndrome coding incorporating some distortion functions is employed, specifically the syndrome-trellis coding (STC) [1] for data embedding and the proposed distortion functions (JC-UED or SI-UED) for embedding efficiency optimization. Fig. 6 illustrates the unified framework for JPEG steganography with original BMP image (Case 1) or JPEG compressed image (Case 2) as input, which includes the process of data embedding and extraction.

A. Data Embedding

1) Preprocessing: The preprocessing is adopted to generate the cover, i.e., the quantized DCT coefficients for data embedding.

Case 1: When input image is original BMP image, the process starts from the implementation of JPEG compression. In this way, the side-information, i.e., the rounding error is

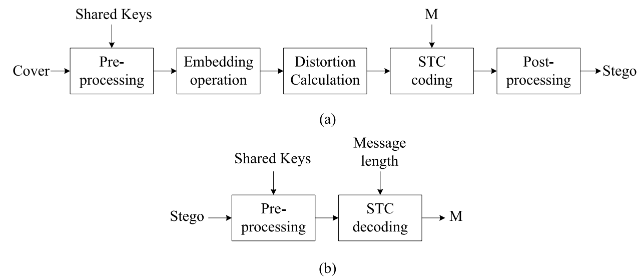


Fig. 6. Proposed scheme. (a) Data embedding. (b) Data extraction.

available for a more secure data embedding. Let $\mathbf{c}' = \{c'_k\}$ and $\mathbf{c} = \{c_k\}$ be the quantized DCT coefficients before and after rounding operation, respectively. Then the rounding error is obtained with $r_k = c_k - c'_k$.

Case 2: When the input image is in JPEG format, the entropy decoding is applied to generate the quantized DCT coefficients $\mathbf{c}$ directly.

In both cases, we obtain the scrambled non-zero AC coefficients $\mathbf{x}$ from $\mathbf{c}$ by a shared key K, i.e.,

$$\mathbf{x} = f_{\mathrm{nz}}(\mathbf{c}, \mathrm{K}) = \{x_k\}, \tag{11}$$

where $f_{\mathrm{nz}}()$ is the mapping function. Similarly $\mathbf{x}' = f_{\mathrm{nz}}(\mathbf{x}', \mathrm{K}) = \{x'_k\}$ denotes the scrambled non-zero AC coefficients before rounding.

2) Embedding Operation: Let $\mathbf{y} = \{y_k\}$ and Δ be the scrambled stego DCT coefficients and embedding operation, respectively. For scrambled AC coefficients $\mathbf{x} = \{x_k\}$, we have $y_k = x_k + \Delta_k$. Before evaluating the distortion of a modified coefficient, the embedding operation Δ itself should be defined.

Case 1: With the original BMP image, the embedding operation Δ is defined as below,

$$\Delta_k = \begin{cases} +1, & \text{if } r_k \le 0 \;\&\; x_k \ne -1 \\ -1, & \text{if } r_k \le 0 \;\&\; x_k = -1 \\ -1, & \text{if } r_k > 0 \;\&\; x_k \ne 1 \\ +1, & \text{if } r_k > 0 \;\&\; x_k = 1 \end{cases}. \tag{12}$$

The embedding error due to data embedding is

$$\begin{aligned} r'_k &= y_k - x'_k \\ &= x_k + \Delta_k - x'_k \\ &= \Delta_k + r_k \\ &= \begin{cases} 1 + r_k, & \text{if } r_k \le 0 \;\&\; x_k \ne -1 \\ -1 + r_k, & \text{if } r_k \le 0 \;\&\; x_k = -1 \\ -1 + r_k, & \text{if } r_k > 0 \;\&\; x_k \ne 1 \\ 1 + r_k, & \text{if } r_k > 0 \;\&\; x_k = 1 \end{cases} \\ |r'_k| &= \begin{cases} 1 - |r_k|, & \text{if } r_k \le 0 \;\&\; x_k \ne -1 \\ 1 + |r_k|, & \text{if } r_k \le 0 \;\&\; x_k = -1 \\ 1 - |r_k|, & \text{if } r_k > 0 \;\&\; x_k \ne 1 \\ 1 + |r_k|, & \text{if } r_k > 0 \;\&\; x_k = 1 \end{cases} \\ &= \begin{cases} 1 + |r_k|, & \text{if } x_k r_k > 0 \;\&\; |x_k| = 1 \\ 1 - |r_k|, & \text{otherwise} \end{cases}. \end{aligned} \tag{13}$$

Thus we have the resulting additional rounding error

$$e_k = |r'_k| - |r_k| = \begin{cases} 1, & \text{if } x_k r_k > 0 \ \& \ |x_k| = 1 \\ 1 - 2|r_k|, & \text{otherwise} \end{cases}. \tag{14}$$

Case 2: When the side-informed original BMP image is not available, the embedding operation Δ is simply defined as

$$\Delta_k = \begin{cases} \mathrm{sgn}(x_i), & \text{if } |x_k| = 1 \\ \pm 1, & \text{if } |x_k| \neq 1 \end{cases}. \tag{15}$$

In both cases, we increase the absolute value of those ± 1 cover coefficients by 1 so that no additional zero DCT coefficients are created.

3) Distortion Calculation: Case 1: Compute the embedding distortion $\rho = \{\rho_k\}$ for each scrambled non-zero AC coefficient x'_k using the SI-UED defined in (10), where the additional rounding error is computed as (14).

Case 2: Compute the embedding distortion $\rho = \{\rho_k\}$ for each scrambled non-zero AC coefficient x_k using the JC-UED defined in (9).

4) STC Coding: Case 1: Since the embedding operation is deterministic as in (12) which is guided by the rounding error, we can only use the binary STC. Let the binary vector $\mathbf{m} = \{m_i\}$ and $\mathbf{x_b} = \{x_{bi}\}$ be the secret message and LSB of cover $\mathbf{x}$, respectively. With $\mathbf{m}$, $\mathbf{x_b}$ and its corresponding embedding cost ρ as input parameters, the binary STC coding [1] is then applied to embed secret message $\mathbf{m}$ to $\mathbf{x}$. The output of STC is the stego $\mathbf{x'_b}$ for $\mathbf{x_b}$, which is then used to construct the modified pattern $\mathbf{p} = \mathrm{xor}(\mathbf{x_b}, \mathbf{x'_b})$ of scrambled non-zero AC coefficients $\mathbf{x}$.

Case 2: Unlike case 1, the embedding operation is non-deterministic as in (15) except that $|x_k| = 1$. Since embedding operation can randomly be $+1$ or -1, this allows us to use the ternary STC to further improve the security performance. With $\mathbf{m}$, $\mathbf{x}$ and its corresponding embedding cost ρ as input parameters, the ternary STC coding [1] is then applied to embed secret message $\mathbf{m}$ to $\mathbf{x}$. And the output of STC is directly the stego $\mathbf{y}$.

5) Postprocessing: Case 1: Once the modified pattern $\mathbf{p} = \mathrm{xor}(\mathbf{x_b}, \mathbf{x'_b})$ is obtained, the cover $\mathbf{x}$ is modified with (16) to obtain stego $\mathbf{y}$. Δ_k is defined in (12).

$$y_k = \begin{cases} x_k, & \text{if } p_k = 0 \\ x_k + \Delta_k, & \text{if } p_k = 1 \end{cases} \tag{16}$$

For both cases, the entropy coding is then applied to generate stego JPEG image after $\mathbf{y}$ is descrambled.

B. Data Extraction

1) Preprocessing: For a stego JPEG image, the quantized DCT coefficients are obtained by entropy decoding, which are then scrambled with the shared key K to generate the scrambled non-zero AC coefficient $\mathbf{y}$.

2) STC Decoding: The STC decoding (binary STC for Case 1 and ternary STC for Case 2) is then applied to extract the secret message $\mathbf{m}$.

V. Experimental Results and Analysis

In this section, experimental results and analysis are presented to demonstrate the feasibility and effectiveness of the proposed UED schemes. The comparisons with several state-of-the-art schemes, such as nsF5 simulator [3], Filler *et al.*'s adaptive scheme with model optimized distortion (MOD) [6] and Holub *et al.*'s J-UNI [10] for non side-informed JPEG steganography, and, Kim *et al.*'s modified matrix encoding (MME) [4], Wang *et al.*'s block entropy weighted scheme (EBS) [7], Sachnev *et al.*'s BCH and BCHopt [5], and Holub *et al.*'s SI-UNI [10] for side-informed JPEG steganography, are included. Note that, in all the involved schemes, with the exception of J-UNI, SI-UNI and BCHopt, other schemes including the proposed UED embed the secret message only to the non-zero AC coefficients and fall into the realm of conventional JPEG Steganography. In our experiments, we concentrate on the comparison of the distortion functions for the involved schemes. Therefore, the Hamming code in MME and BCH code in BCH are replaced with STC in the interest of fair comparison. Moreover, the proposed SI-UED will utilize both STC and BCH code when compared with BCHopt in [5].

A. Experiment Setup

All experiments are carried out on the image database BOSSbase [15]. The original database contains 10,000 images acquired by eight digital cameras in their RAW format (CR2 or DNG) and subsequently processed by converting to grayscale, and then resizing and cropping to the size of 512×512 pixels using the script available from [15]. The images in BOSSbase are then JPEG compressed using quality factors 75, 85 and 95. Thus, we have four image databases each with 10,000 grayscale cover images of different texture characteristics in format of BMP and JPEG, which serve as the precover (BMP) and cover (JPEG) for side-informed and non side-informed JPEG embedding, respectively. In our experiments, the payloads for both non side-informed and side-informed embedding range from 0.1 to 0.5 bpac with a step of 0.1. Several mainstream universal feature sets for JPEG steganalysis, such as the CC-PEV-548D [8], MP-486D [13] and the state-of-the-art CC-JRM-22,510D [11], are employed to evaluate the security performances of the involved JPEG steganographic schemes. Considering the proposed UED tends to spread the embedding to all possible quantized DCT coefficients with different magnitude, the IBC-EM-882D feature set in [9], which focuses on detecting the embedding changes to DCT coefficients with a large magnitude, is also included in our experiments.

The ensemble classifier in [12] is incorporated in our experiments as is done in [11], since it enables fast training in high-dimensional feature spaces and has a comparable performance to that of SVMs [18] working on low-dimensional feature sets. Considering the CC-PEV-548D, MP-486D and IBC-EM-882D are originally designed for SVM, we also utilize the SVM as the classifier for these three feature sets. The parameters of SVM are set as in [8], [9], and [13], respectively. For the cover and their corresponding stego images with different steganographic schemes, embedding rates and

TABLE I

DETECTION ERRORS FOR THE INVOLVED NON SIDE-INFORMED AND SIDE-INFORMED SCHEMES ON BOSSBASE WITH CC-PEV-548D, MP-486D AND IBC-EM-882D, AND ENSEMBLE AND SVM CLASSIFIERS FOR QUALITY FACTORS 75

Algorithm	Payload	Non side-informed					Side-informed (STC coded)					Side-informed (BCH coded)	
		nsF5	MOD	J-UNI	SC-UED	JC-UED	MME	BCH	EBS	SI-UNI	SI-UED	BCHopt	SI-UED
Ensemble + CC-PEV-548D	0.10	0.2577	0.3870	0.4726	0.4211	0.4292	0.4354	0.4541	0.4795	0.5000	0.4868	0.4453	0.4736
	0.20	0.0773	0.2841	0.4155	0.2856	0.3241	0.2342	0.3163	0.4068	0.4947	0.4356	0.3111	0.4064
	0.30	0.0207	0.1775	0.3467	0.1398	0.1933	0.0295	0.1562	0.2728	0.4813	0.3348	0.1382	0.2563
	0.40	0.0061	0.0890	0.2737	0.0434	0.0888	0.0015	0.0451	0.1217	0.4506	0.1978	–	–
	0.50	0.0027	0.0329	0.2018	0.0102	0.0294	0.0001	0.0061	0.0255	0.4196	0.0546	–	–
Ensemble + MP-486D	0.10	0.3584	0.4244	0.4940	0.4760	0.4819	0.4516	0.4726	0.4884	0.5000	0.4975	0.4675	0.4921
	0.20	0.1966	0.3462	0.4807	0.3878	0.4297	0.2873	0.3768	0.4344	0.4967	0.4735	0.3709	0.4545
	0.30	0.0940	0.2904	0.4530	0.2568	0.3267	0.0570	0.2380	0.3321	0.4834	0.4135	0.2200	0.3523
	0.40	0.0467	0.2283	0.4131	0.1227	0.2108	0.0045	0.1000	0.1810	0.4726	0.3041	–	–
	0.50	0.0242	0.1403	0.3519	0.0376	0.1063	0.0006	0.0214	0.0536	0.4447	0.1291	–	–
Ensemble + IBC-EM-882D	0.10	0.3639	0.0352	0.4976	0.4710	0.4829	0.4519	0.4728	0.4866	0.4997	0.4954	0.4668	0.4884
	0.20	0.2111	0.0244	0.4894	0.3716	0.4201	0.2939	0.3727	0.4671	0.4978	0.4825	0.3692	0.4534
	0.30	0.1067	0.0245	0.4663	0.2352	0.3206	0.0930	0.2525	0.4005	0.4915	0.4448	0.2113	0.3442
	0.40	0.0533	0.0261	0.4322	0.1107	0.2087	0.0158	0.1579	0.2759	0.4807	0.3664	–	–
	0.50	0.0295	0.0240	0.3864	0.0400	0.1187	0.0026	0.0841	0.1389	0.4627	0.2636	–	–
SVM + CC-PEV-548D	0.10	0.2724	0.4084	0.4812	0.4471	0.4563	0.4366	0.4588	0.4852	0.4935	0.4947	0.4481	0.4818
	0.20	0.0962	0.3252	0.4401	0.3148	0.3617	0.2377	0.3287	0.4197	0.4938	0.4631	0.3184	0.4180
	0.30	0.0277	0.2284	0.3786	0.1657	0.2372	0.0322	0.1609	0.2735	0.4833	0.3781	0.1447	0.2694
	0.40	0.0097	0.1382	0.3042	0.0648	0.1200	0.0019	0.0557	0.1310	0.4648	0.2432	–	–
	0.50	0.0032	0.0652	0.2309	0.0200	0.0494	0.0002	0.0101	0.0344	0.4320	0.0877	–	–
SVM + MP-486D	0.10	0.3372	0.4098	0.4902	0.4645	0.4728	0.4466	0.4711	0.4852	0.4951	0.4910	0.4677	0.4881
	0.20	0.1714	0.3262	0.4764	0.3588	0.4096	0.2757	0.3731	0.4327	0.4922	0.4700	0.3707	0.4506
	0.30	0.0785	0.2618	0.4452	0.2209	0.3034	0.0485	0.2311	0.3207	0.4848	0.4073	0.2106	0.3274
	0.40	0.0364	0.1866	0.3994	0.0961	0.1846	0.0062	0.0854	0.1704	0.4682	0.2832	–	–
	0.50	0.0174	0.1161	0.3280	0.0331	0.0881	0.0012	0.0058	0.0402	0.4361	0.1026	–	–
SVM + IBC-EM-882D	0.10	0.3536	0.0376	0.4930	0.4644	0.4761	0.4563	0.4771	0.4845	0.4981	0.4889	0.4730	0.4848
	0.20	0.2013	0.0248	0.4856	0.3473	0.4038	0.3061	0.3807	0.4759	0.4940	0.4842	0.3805	0.4498
	0.30	0.0969	0.0258	0.4650	0.2010	0.2986	0.0996	0.2577	0.4106	0.4874	0.4312	0.2228	0.3405
	0.40	0.0477	0.0229	0.4356	0.0965	0.1894	0.0207	0.1539	0.2791	0.4884	0.3459	–	–
	0.50	0.0236	0.0201	0.3872	0.0349	0.1034	0.0045	0.0842	0.1371	0.4672	0.2348	–	–

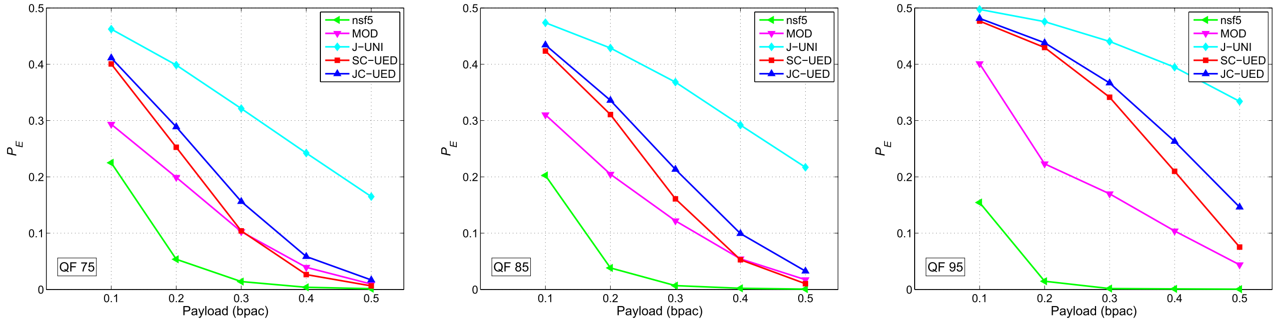
QFs, the feature sets for the involved steganalysis tools are extracted, where half of the cover and the stego features are used as the training set for both the ensemble and SVM classifiers, and the remaining half are used as test set to evaluate the trained classifier. The minimal total error P_{E} under equal priors achieved on the test set is defined as

$$P_{\mathrm{E}} = \min_{P_{\mathrm{FA}}} \frac{P_{\mathrm{FA}} + P_{\mathrm{MD}}(P_{\mathrm{FA}})}{2}, \tag{17}$$

where P_{FA} is the false alarm rate and P_{MD} is the missed detection rate. The performance is evaluated using the median value of P_{E} over ten random tests and is denoted as $\bar{P}_E$.

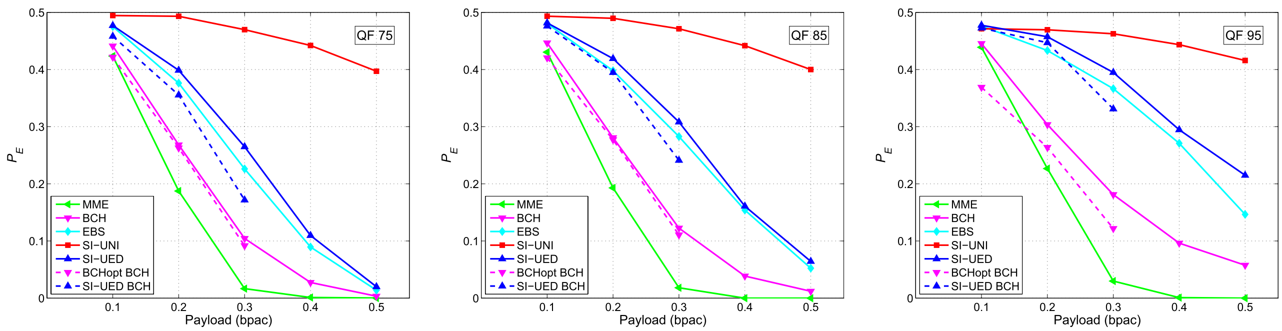
B. Performance of Non Side-Informed UED

For JPEG steganography without side-information, we compare the proposed SC-UED and JC-UED with nsF5 [3], MOD [6] and the recently proposed J-UNI [10]. The security performances of the involved schemes against the CC-JRM-22,510D, for JPEG quality factors 75, 85 and 95, are illustrated in Fig. 7. For all cases, J-UNI achieves the best security performance as expected, while JC-UED clearly outperforms nsF5 as well as MOD by a sizeable margin across all three quality factors. We also report in Table I the security performances of the involved non side-informed and side-informed schemes against the CC-PEV-548D, MP-486D and IBC-EM-882D, with both ensemble and SVM classifiers, for JPEG quality factor 75. Again, for all cases, J-UNI achieves the best security performance. For CC-PEV-548D and MP-486D with both ensemble and SVM classifiers, both JC-UED and SC-UED have considerably better performance than that of nsF5 for all tested payloads, and JC-UED outperforms MOD for medium and



(a) (b) (c)

Fig. 7. Detection errors as a function of relative payload for nsF5, MOD, J-UNI, SC-UED and JC-UED on BOSSbase with CC-JRM-22,510D and ensemble classifier for (a) QF = 75, (b) QF = 85 and (c) QF = 95. MOD, J-UNI, SC-UED and JC-UED are ternary STC coded.



(a) (b) (c)

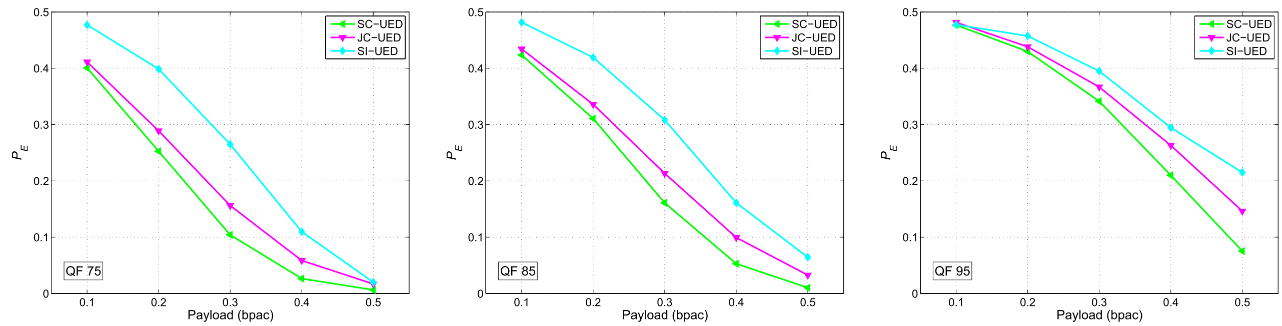
Fig. 8. Detection errors as a function of relative payload for MME , BCH , BCHopt, EBS, SI-UNI and SI-UED on BOSSbase with CC-JRM-22,510D and ensemble classifier for (a) QF = 75, (b) QF = 85 and (c) QF = 95. MME, BCH, EBS and SI-UNI are binary STC coded, BCHopt is BCH coded, and SI-UED is both binary STC and BCH coded.

low payloads. It is noted that the MOD is optimized to CC-PEV-548D [8]. Even under this circumstance, the JC-UED still has a better performance than the one of MOD for most of the tested payloads, and is only slightly outperformed by MOD for large data payload (≥0.4 bpac) when both JC-UED and MOD can be reliably detected by CC-PEV-548D. Table I also shows the performance of the involved non side-informed schemes against the feature set IBC-EM-882D [9], which consists of the enlarged inter-block co-occurrence and the extended Markov features by increasing the corresponding threshold T, respectively, which are devised to detect the embedding changes in DCT coefficients with a large magnitude. It is observed that, for various payloads, JC-UED, SC-UED, J-UNI and nsF5 with IBC-EM-822D can achieve a better and comparable performance than their corresponding ones with CC-PEV-548D and MP-486D, whereas the performance of MOD can fall significantly when IBC-EM-822D is applied, suggesting that: 1) the distortion function in MOD is somewhat overtraining to the incomplete cover model CC-PEV-548D and can be reliably detected by the IBC-EM features; 2) the proposed UED spreads uniformly its embedding changes to all possible quantized DCT coefficients with different magnitude and thus leads to much less sudden changes even for those coefficients with relatively large magnitude. It is readily seen from Table I that, for IBC-EM-882D, the proposed JC-UED and SC-UED work considerably better than nsF5, while the MOD can still be reliably detected for all the tested payloads.

It is noted that the proposed distortion function in JC-UED uses only coefficients in DCT domain without transformation to other domains, while the J-UNI uses spatial domain distortion for JPEG steganography, which is quite time-consuming. In addition, unlike the conventional approaches, the J-UNI uses all DCT coefficients as possible cover elements, and a sizeable proportion of DC and zero AC coefficients are incorporated in the J-UNI for JPEG steganography. J-UNI currently seems to work better, perhaps because there are no features yet that would detect it, especially those changes in DC and zero AC coefficients. Therefore, at least, in the "framework of conventional JPEG steganography", the proposed JC-UED method can still provide the best security performance.

C. Performance of Side-Informed UED

For JPEG steganography with side-information, we compare the proposed SI-UED with MME [4], BCH [5], BCHopt [5], EBS [7] and recently proposed SI-UNI [10]. Fig. 8 shows the security performance of the involved schemes against the CC-JRM-22,510D, for JPEG quality factors 75, 85 and 95. Note that the schemes in Fig. 8(a)–(c) are all binary STC coded except the BCHopt for fair comparison. By 'BCH' and



(a) (b) (c)

Fig. 9. Detection errors as a function of relative payload for SC-UED, JC-UED and SI-UED on BOSSbase with CC-JRM-22,510D and ensemble classifier for (a) QF = 75, (b) QF = 85 and (c) QF = 95. SC-UED and JC-UED are ternary STC coded, while SI-UED is binary STC coded.

'BCHopt', we mean the baseline distortion function and its enhanced version used in [5] for non zero AC coefficients and all possible AC coefficients (non-zero and zero ACs), respectively. As in the non side-informed case, the SI-UNI achieves the best security performance for almost all cases except that it is slightly outperformed by the SI-UED when the payload is 0.10 bpac for JPEG quality factor 95, while the proposed SI-UED has a significantly better performance than the ones of MME and BCH and outperforms EBS by a clear margin for all tested payloads. Note that BCHopt can only be implemented with fast BCH syndrome coding and has long been known as one of the most secure side-informed steganographic schemes for its heuristic optimization [5]. To verify the superiority of SI-UED is irrelevant to the used code, Fig. 8(a)–(c) further compare the SI-UED with BCHopt when both of the schemes are BCH coded. Again, the SI-UED performs much better than BCHopt for all tested payloads across all three quality factors. We also report the security performances of the involved side-informed schemes against the CC-PEV-548D, MP-486D and IBC-EM-882D, for JPEG quality factor 75 in Table I. Again SI-UNI achieves the best security performance, and the SI-UED outperforms all other schemes when encoded with binary STC, and also outperforms the BCHopt when encoded with BCH code for all tested payloads and classifiers.

The pros and cons between SI-UED and SI-UNI are similar to the ones between JC-UED and J-UNI as described in Section V.B.

Fig. 9 illustrates the performance comparison of the non side-informed SC-UED and JC-UED, and the side-informed SI-UED, against the feature set CC-JRM-22,510D with quality factors 75, 85 and 95. For almost all the cases, the SI-UED with binary STC achieves the best performance, even though the SC-UED and JC-UED are both ternary STC coded, indicating that the precover as side information may contribute more to the improvement of the security performance than simply increasing the coding efficiency by using M-ary Code.

VI. Conclusion

Minimal-distortion embedding framework is a practical approach to implement JPEG steganography with high embedding efficiency. In this paper, an efficient JPEG steganographic scheme which utilizes syndrome trellis coding (STC) and uniform embedding (UE) strategy is presented. The uniform embedding is similar in spirit to spread spectrum communication. By uniformly "spreading" the embedding modifications to quantized DCT coefficients of all possible magnitudes, the average changes of first- and second-order statistics are possibly minimized, especially in the small coefficients, which leads to less statistical detectability, and hence, more secure steganography. A class of new distortion functions known as uniform embedding distortion function (UED) for both non side-informed and side-informed JPEG steganography are developed to incorporate the uniform embedding. The JC-UED for non side-informed embedding takes into account the magnitude of DCT coefficient as well as both its intra- and inter-block neighborhood coefficients, while the SI-UED for side-informed embedding further explores the additional rounding error besides the requirement of uniform embedding. Extensive experiments have been carried out to demonstrate the superior performance of the proposed scheme in terms of secure embedding payload against steganalysis.

Finally, it is worthwhile to note that, the inappropriate use of DC and zero AC coefficients in JPEG steganography may lead to additional block artifacts in stego image and decrease in the efficiency of JPEG compression, respectively. That is why the most existing JPEG steganographic schemes use only non-zero AC coefficients as possible cover elements to make the embedding naturally content-adaptive. With the carefully devised distortion function, however, the embedding should be made "artificially" content-adaptive in principle. According to some of our experiments, some DC and zero AC coefficients in the texture regions could indeed be incorporated to further data embedding without decreasing, even increasing the security performance. While the UED proposed in this paper could by no means tackle all of these issues, it raises a quite challenging open question, that is how to evaluate the embedding costs of all possible DCT coefficients (including DCs, zero and non-zero ACs) based solely on the coefficients in the DCT domain for JPEG steganography, which remains as the topic of our future research effort.

Acknowledgment

The authors would like to thank the anonymous reviewers and associate editor for their comments that greatly improved the manuscript.

REFERENCES

[1] T. Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 920–935, Sep. 2011.

[2] A. Westfeld, "F5—A steganographic algorithm," in *Proc. 4th Inf. Hiding Conf.*, vol. 2137. 2001, pp. 289–302.

[3] J. Fridrich, T. Pevný, and J. Kodovský, "Statistically undetectable JPEG steganography: Dead ends challenges, and opportunities," in *Proc. 9th ACM Workshop Multimedia Security*, Dallas, TX, USA, Sep. 2007, pp. 3–14.

[4] Y. Kim, Z. Duric, and D. Richards, "Modified matrix encoding technique for minimal distortion steganography," in *Proc. 8th Inf. Hiding Conf.*, vol. 4437. Jul. 2006, pp. 314–327.

[5] V. Sachnev, H. J. Kim, and R. Zhang, "Less detectable JPEG steganography method based on heuristic optimization and BCH syndrome coding," in *Proc. 11th ACM Workshop Multimedia Security*, Sep. 2009, pp. 131–140.

[6] T. Filler and J. Fridrich, "Design of adaptive steganographic schemes for digital images," *Proc. SPIE*, vol. 7880, p. 78800F, Jan. 2011.

[7] C. Wang and J. Ni, "An efficient JPEG steganographic scheme based on the block entropy of DCT coefficients," in *Proc. IEEE ICASSP*, Kyoto, Japan, Mar. 2012, pp. 1785–1788.

[8] J. Kodovský and J. Fridrich, "Calibration revisited," in *Proc. 11th ACM Workshop Multimedia Security*, New York, NY, USA, Sep. 2009, pp. 63–74.

[9] J. Kodovský, J. Fridrich, and V. Holub, "On dangers of overtraining steganography to incomplete cover model," in *Proc. 13th ACM Workshop Multimedia Security*, New York, NY, USA, Sep. 2011, pp. 69–76.

[10] V. Holub and J. Fridrich, "Digital image steganography using universal distortion," in *Proc. 1st ACM Workshop Inf. Hiding Multimedia Security*, 2013, pp. 59–68.

[11] J. Kodovský and J. Fridrich, "Steganalysis of JPEG images using rich models," *Proc. SPIE*, vol. 8303, p. 83030A, Jan. 2012.

[12] J. Kodovský, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 432–444, Apr. 2012.

[13] C. Chen and Y. Q. Shi, "JPEG image steganalysis utilizing both intrablock and interblock correlations," in *Proc. IEEE Int. Symp. Circuits Syst.*, Mar. 2008, pp. 3029–3032.

[14] L. Guo, J. Ni, and Y. Q. Shi, "An efficient JPEG steganographic scheme using uniform embedding," in *Proc. 4th IEEE Int. Workshop Inf. Forensics Security*, Tenerife, Spain, Dec. 2012, pp. 169–174.

[15] P. Bas, T. Filler, and T. Pevný, "Break our steganographic system—The ins and outs of organizing boss," in *Proc. 13th Inf. Hiding Conf.*, 2011, pp. 59–70.

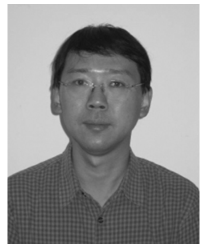
[16] N. Provos, "Defending against statistical steganalysis," in *Proc. 10th USENIX Security Symp.*, Washington, DC, USA, 2001, pp. 323–335.

[17] D. Freedman, *Statistical Models: Theory and Practice*. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[18] C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," *ACM Trans. Intell. Syst. Technol.*, vol. 2, no. 3, pp. 27:1–27:27, 2011.

Linjie Guo (S'12) received the B.S. degree in engineering from the South China University of Technology, Guangzhou, China, in 2010. He is currently pursuing the Ph.D. degree with the School of Information Science and Technology, Sun Yat-sen University, Guangzhou.

His current research interests include steganography, steganalysis, and multimedia security.



Jiangqun Ni (M'12) received the Ph.D. degree in electronic engineering from the University of Hong Kong, Hong Kong, in 1998.

He was a Post-Doctoral Fellow for a joint program between the Sun Yat-sen University, Guangzhou, China, and the Guangdong Institute of Telecommunication Research from 1998 to 2000. Since 2001, he has been with the School of Information Science and Technology, Sun Yat-sen University, where he is currently a Professor. His research interests include data hiding and digital image forensics, image-based modeling and rendering, and image/video processing. He has authored more than 50 papers in these areas.

Yun Qing Shi (M'88–SM'92–F'05) has been with the New Jersey Institute of Technology, USA, since 1987. He received the M.S. degree from Shanghai Jiao Tong University, China, and the Ph.D. degree from the University of Pittsburgh, USA. His research interests include digital data hiding, forensics and information assurance, and visual signal processing and communications.

He has authored and coauthored more than 300 papers, one book, and five book chapters, and has edited 10 books. He holds 28 U.S. patents. He received the Innovators Award 2010 from the New Jersey Inventors Hall of Fame for Innovations in Digital Forensics and Security. His U.S. patent 7,457,341 titled "System and Method for Robust Reversible Data Hiding and Data Recovery in the Spatial Domain" received the 2010 Thomas Alva Edison Patent Award from the Research and Development Council of New Jersey.

He served as an Associate Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING and IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS (II), and a few other journals, the Technical Program Chair of the 2007 IEEE International Conference on Multimedia and Expo, a Co-Technical Chair of the 2006, 2007, and 2009–2013 International Workshop on Digital Watermarking, and the 2005 IEEE International Workshop on Multimedia Signal Processing (MMSP), a Co-General Chair of the 2002 IEEE MMSP, and a Distinguished Lecturer of the IEEE Circuits and Systems Society. He is a member of a few IEEE technical committees.