Minimum Perturbation Cost Modulation for Side-Informed Steganography

Jan Butora and Jessica Fridrich, Department of ECE, SUNY Binghamton, NY, USA, {jbutora1, fridrich}@binghamton.edu

Abstract

A new rule for modulating costs in side-informed steganography is proposed. The modulation factors of costs are determined by the minimum perturbation of the precover to quantize to the desired stego value. This new rule is contrasted with the established way of weighting costs by the difference between the rounding errors to the cover and stego values. Experiments are used to demonstrate that the new rule improves security in ternary side-informed UNIWARD in JPEG domain. The new rule arises naturally as the correct cost modulation for JPEG side-informed steganography with the "trunc" quantizer used in many portable digital imaging devices.

Introduction

Side-informed steganography is a form of covert communication in which a secret message is embedded in a cover object during processing (or conversion) of a precover [13] to cover. For example, the sender can make use of the fact that she has the uncompressed image before applying JPEG compression. In this case, the rounding errors e_{ij} during quantization of DCT (Discrete Cosine Transform) coefficients form the side-information. The actual embedding of the secret message occurs jointly during processing the precover. Intuitively, DCT coefficients with rounding errors $|e_{ij}| \approx 1/2$ are the most "unstable" in the sense that a small amount of noise could cause them to be rounded to a different value during compression. In side-informed steganography, such coefficients are given a smaller embedding cost to minimize the overall statistical impact of embedding changes.

Side-information can have many forms and can be applied whenever a high quality precover is available to the sender who applies to it some information-reducing processing to obtain the cover as long as the last step of the processing is quantization. Examples include converting a true-color image to a palette format [7], JPEG recompression [8], and the by far most popular case of JPEG compression [17, 19, 21, 12, 11, 10, 4].

Originally, side-informed schemes were inherently *binary* in the sense that the only embedding changes allowed were those in which the cover element (before rounding) was "rounded to the second closest value." The authors of [4] showed the benefit of ternary embedding by allowing embedding changes by ± 1 with appropriately modulated costs. The authors noted that the benefit of ternary embedding over binary is larger for fine quantization, e. g., in the spatial domain, and comparatively much smaller for harsh quantization (in JPEG domain). As this paper indicates, this is likely due to not penalizing the cost of the "furthest" (third) stego value enough. To this end, we propose a new heuristic rule for modulating costs based on the minimum perturbation that needs to be applied to the precover to round to the desired stego value. The benefit of this rule is especially apparent when the quantization is harsh. It also universally applies when the quantizer is simple rounding as well as when the quantizer is truncation towards zero as is the case for some JPEG compressors.

In the next section, we review previous art in binary and ternary side-informed steganography. In the third section, we introduce the new rule for cost modulation, and the following section contains the results of all experiments and their interpretation. The paper is concluded in the last section.

Modulating costs (prior art)

For steganography designed to minimize costs (embedding distortion), a popular heuristic to incorporate a precover value $x_{ij} \in \mathbb{R}$ during embedding is to modulate the costs based on the quantization error, which is in case of rounding, $e_{ij} = x_{ij} - [x_{ij}]$, $-1/2 \leq e_{ij} \leq 1/2$ [17, 21, 12, 10, 11, 4, 19], where $[\cdot]$ denotes the operation of rounding to the nearest integer.

Binary side-informed embedding

A binary embedding scheme modulates the cost of changing $c_{ij} = [x_{ij}]$ to $[x_{ij}] + \mathrm{sign}(e_{ij})$ by $1-2|e_{ij}|$, while prohibiting the change to $[x_{ij}] - \mathrm{sign}(e_{ij})$:

$$\rho_{ij}^{(\mathrm{B})}(\mathrm{sign}(e_{ij})) = (1-2|e_{ij}|)\rho_{ij} \quad (1)$$

$$\rho_{ij}^{(\mathrm{B})}(-\mathrm{sign}(e_{ij})) = \Omega, \quad (2)$$

where $\rho_{ij}^{(\mathrm{B})}(u)$ is the cost of modifying the cover value by $u \in \{-1, 1\}$, ρ_{ij} are costs of some additive embedding scheme, and Ω is a large constant ("wet" cost [9]). The superscript B indicates that the costs are for binary embedding. This modulation is usually justified heuristically because when $|e_{ij}| \approx 1/2$, a small perturbation of x_{ij} could cause c_{ij} to be rounded to the other side. Such coefficients are thus assigned a proportionally smaller cost because $1-2|e_{ij}| \approx 0$. On the other hand, the costs are unchanged when $e_{ij} \approx 0$.

The factor $1-2|e_{ij}|$ for cost modulation has been studied in [5], where the authors showed that, based on a discrete Gaussian precover model, the steganographic Fisher information should be modulated by the square of the same

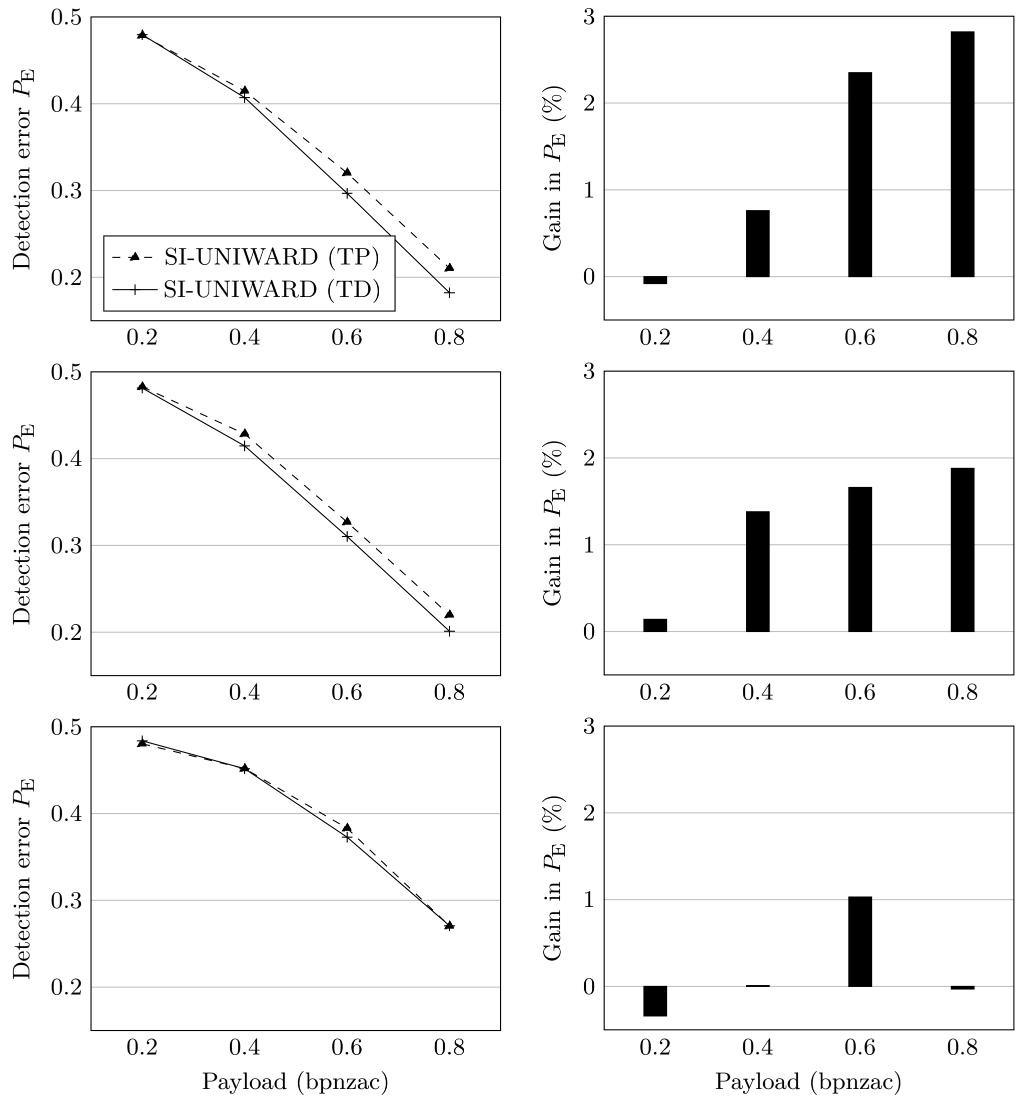

Figure 1. *By rows: Detection error P_{E} of SCA-GFR / GFR for SI-UNIWARD with (old) cost modulation by difference (TD) (solid) and (new) modulation by minimum perturbation (TP) (dashed) at quality factors 75, 85, and 95 (left). The right column shows the increase of P_{E} when going from (TD) to (TP) modulations.*

factor. This provides some justification to the heuristics in this paper and also in previous art.

Ternary side-informed embedding

A ternary version of this embedding strategy [4] allows modifications both ways with costs :

$$\rho_{ij}^{(\mathrm{TD})}(\mathrm{sign}(e_{ij})) = (1-2|e_{ij}|)\rho_{ij} \tag{3}$$

$$\rho_{ij}^{(\mathrm{TD})}(-\mathrm{sign}(e_{ij})) = \rho_{ij}. \tag{4}$$

The modulation factors $1-2|e_{ij}|$ and 1 are the differences between the rounding errors to a stego element $y_{ij} \in \{[x_{ij}]-1, [x_{ij}]+1\}$ and to the cover element :

$$\eta_{ij} = |y_{ij} - x_{ij}| - |x_{ij} - [x_{ij}]|. \tag{5}$$

Indeed, when $y_{ij} = [x_{ij}] + \mathrm{sign}(e_{ij})$, $\eta_{ij} = 1 - 2|e_{ij}|$. When $y_{ij} = [x_{ij}] - \mathrm{sign}(e_{ij})$, $\eta_{ij} = 1 + |e_{ij}| - |e_{ij}| = 1$, in agreement with (3)–(4). The superscript TD stands for **T**ernary cost modulation by **D**ifference. Note that the cost either stays the same or *decreases*, while the sum of both costs is

$$\rho_{ij}^{(\mathrm{TD})}(-1) + \rho_{ij}^{(\mathrm{TD})}(+1) = 2\rho_{ij} - 2|e_{ij}|\rho_{ij}, \tag{6}$$

and is thus dependent on the rounding error e_{ij}. In the next section, we replace the rule with an alternative rule that assigns larger costs to changes by $-\mathrm{sign}(e_{ij})$, while it assigns the same cost to changes by $\mathrm{sign}(e_{ij})$ as in (3).

Cost modulation by minimum perturbation

The proposed rule can be simply worded in English by stating that the modulation factor is the minimum amount

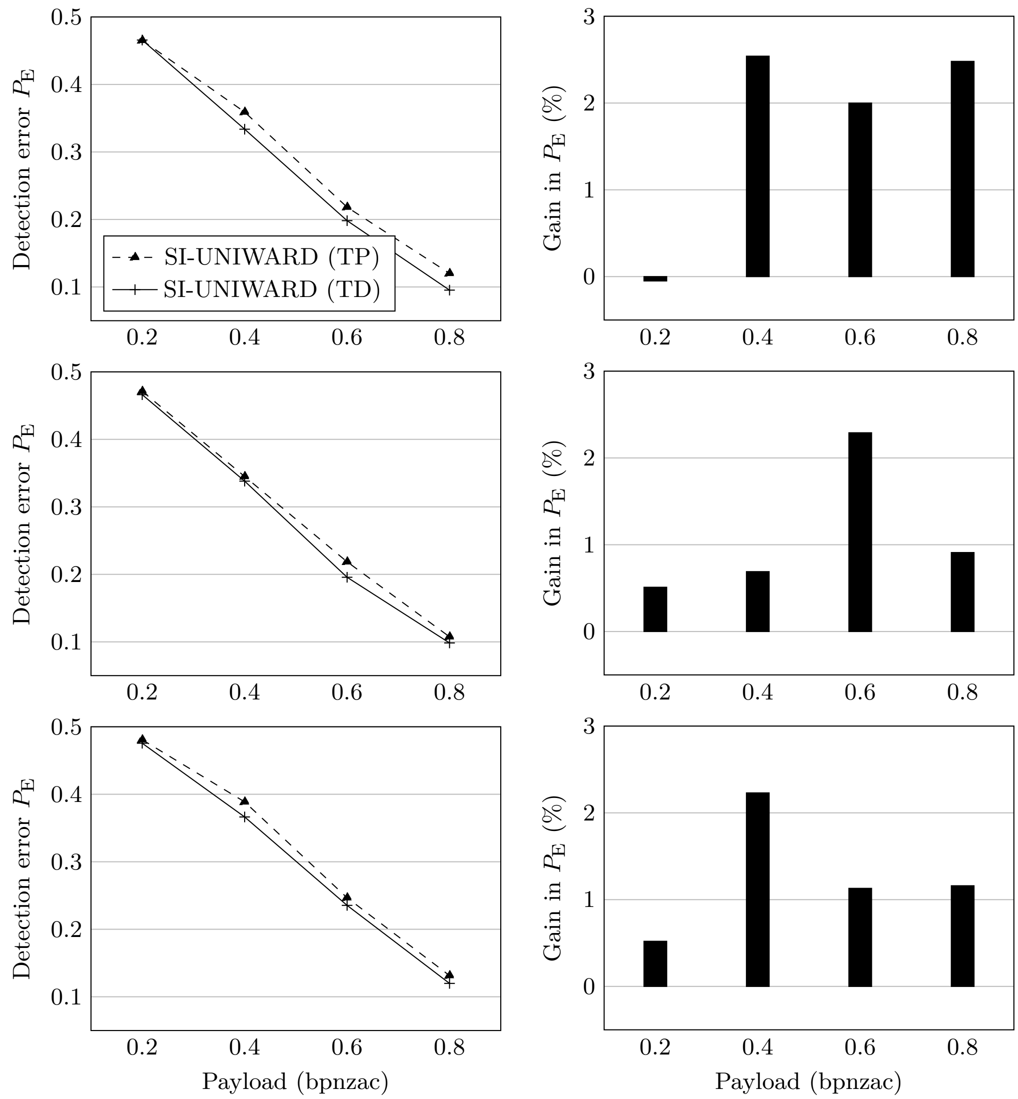

Figure 2. *By rows: Detection error P_{E} of SCA-SRNet / SRNet for SI-UNIWARD with (old) cost modulation by difference (TD) (solid) and (new) modulation by minimum perturbation (TP) (dashed) at quality factors 75, 85, and 95 (left). The right column shows the increase of P_{E} when going from (TD) to (TP) modulations.*

of perturbation applied to the precover to quantize to the desired value. This minimum perturbation is $1/2-|e_{ij}|$ for change $[x_{ij}]\to[x_{ij}]+\mathrm{sign}(e_{ij})$ and $1/2+|e_{ij}|$ for $[x_{ij}]\to[x_{ij}]-\mathrm{sign}(e_{ij})$:

$$\rho_{ij}^{(\mathrm{TP})}(\mathrm{sign}(e_{ij})) = (1/2-|e_{ij}|)\rho_{ij} \tag{7}$$

$$\rho_{ij}^{(\mathrm{TP})}(-\mathrm{sign}(e_{ij})) = (1/2+|e_{ij}|)\rho_{ij}. \tag{8}$$

The superscript TP stands for **T**ernary cost modulation by minimum **P**erturbation. Since multiplying all costs by the same scalar does not change the properties of the embedding scheme, notice that the modulation factors can equivalently be $1-2|e_{ij}|$ and $1+2|e_{ij}|$, respectively. In contrast to the established way of cost modulation in side-informed steganography, rounding "against" the rounding error is now penalized more. Thus, one can expect that this will have the biggest impact for harsh quantization (low quality JPEG). Also note that the sum of costs is now equal to the sum of the original costs

$$\rho_{ij}^{(\mathrm{TP})}(-1)+\rho_{ij}^{(\mathrm{TP})}(+1) = 2\rho_{ij}. \tag{9}$$

Experiments

This section contains the results of all experiments and their interpretation. We begin with SI-UNIWARD with the round quantizer and contrast the old (TD) cost modulation with the new one (TP). Then, we focus on "trunc" JPEGs and use the new rule for cost modulation in SI-UNIWARD (the old rule is inapplicable in this source).

Dataset

Our dataset was derived from 47,260 RAW images provided as part of the steganalysis competition ALASKA.[1] Available from the same web site is the script for developing the RAW images to the true-color (24 bit) TIFF format.[2] Then, the image was converted to grayscale, leaving the pixel values represented as "double," and resized using the cubic kernel so that the smaller side is 256, and finally centrally cropped to 256×256. The reader is referred to the above-cited ALASKA web site for more information the script. Pixel values were stored as integers before compression.

The database was randomly split into training, validation, and testing sets with 40,460, 3,200, and 3,600 images. Detectors trained as classifiers with rich models were trained on the union of the training and validation sets.

Evaluation metric

The detection performance was measured with the total classification error under equal priors on the test set

$$P_{\mathrm{E}} = \min_{P_{\mathrm{FA}}} \frac{1}{2}(P_{\mathrm{FA}} + P_{\mathrm{MD}}), \tag{10}$$

where P_{FA} and P_{MD} stand for the false-alarm and missed-detection probabilities.

Round JPEGs

Table 1 and Figures 1, 2 contrast the performance of ternary SI-UNIWARD as proposed in [4] (with TD modulation of costs) and the proposed version with costs modulated by minimum perturbation (TP). The tested payloads were 0.2, 0.4, 0.6, and 0.8 bits per non-zero AC DCT coefficient (bpnzac). While the impact of the new cost modulation is the largest for low quality factors and large payloads, improvement in security is observed for every tested scenario, with the exception of the largest quality factor 95 with payload 0.8 bpnzac, where the schemes attain the same level of detectability, and for quality factors 75 and 95 with payload 0.2 where the algorithms are virtually undetectable. In particular, with the selection-channel-aware (SCA) GFR feature set [20, 3], for quality 75, the improvement in security is almost 3% in terms of P_{E} for the largest payload. This gain decreases to 1.5–2% for quality 85. For the highest tested quality of 95, the improvement was less than 1%.

The selection channel supplied to the SCA-SRNet was computed from the non-modulated costs because the modulation (side-information) is not available to the steganalyst. Interestingly, in most cases the selection channel actually hurts the performance of the SRNet. We conjecture that this may be due to the imprecise selection channel. The improvement in security offered by the new modulation is consistent with what was observed with rich models.

[1] `https://alaska.utt.fr`

[2] We modified the conversion script to only use the 'dem_amaze.pp3' RAW converter.

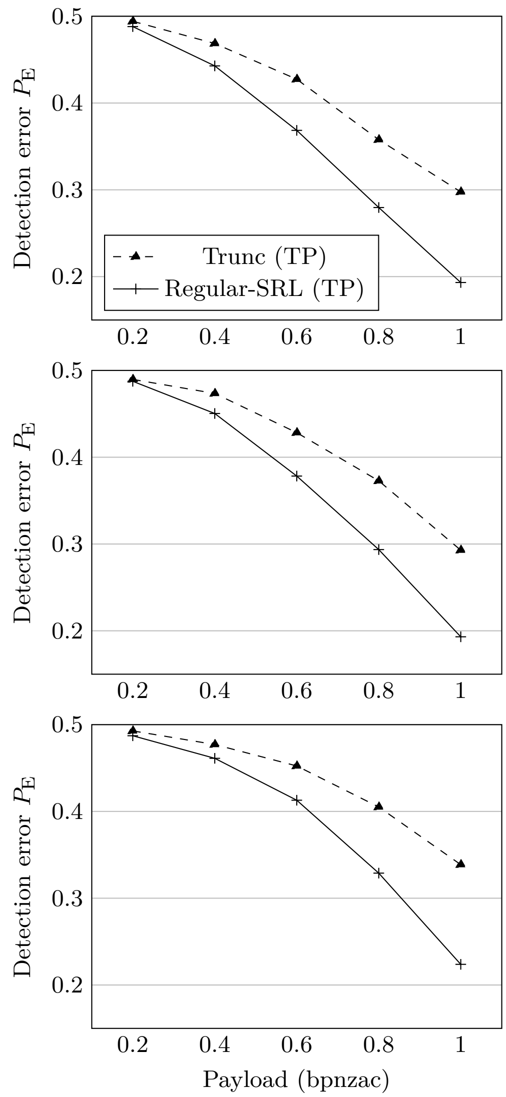

Figure 3. Detection error P_{E} of GFR for SI-UNIWARD with (new) modulation by minimum perturbation (TP) in trunc JPEGs (dashed) and with standard JPEGs with payload correction according to SRL (solid) at quality factors 75, 85, and 95.

The trunc quantizer

Many portable imaging devices today use a slightly different implementation of JPEG compression that employs the operation of truncation for quantizing DCT coefficients [1, 2]. This quantizer essentially rounds towards zero instead of the nearest integer. Formally, the precover value x_{ij} is quantized to the nearest integer smaller than or equal to x_{ij} when $x_{ij} \geq 0$, and to the nearest integer larger than or equal to x_{ij} when $x_{ij} < 0$. This way of quantizing is adopted probably due to an easier hardware implementation.

Applying the original (TD) rule for modulation in this source leads to obvious problems because the rounding error $0 \leq e_{ij} < 1$ for $x_{ij} > 0$ and $-1 < e_{ij} \leq 0$ for $x_{ij} < 0$. A modulation factor $1 - 2|e_{ij}|$ would thus lead to negative

Detector	Modulation	QF 75				QF 85				QF 95			
		0.2	0.4	0.6	0.8	0.2	0.4	0.6	0.8	0.2	0.4	0.6	0.8
GFR	TD	**0.4796**	0.4071	0.2968	0.1822	0.4814	0.4147	0.3103	0.2011	**0.4838**	0.4517	0.3728	**0.2707**
	TP	0.4788	**0.4147**	**0.3203**	**0.2104**	**0.4828**	**0.4285**	**0.3269**	**0.2199**	0.4804	**0.4518**	**0.3831**	0.2704
SRNet	TD	**0.4658**	0.3337	0.1982	0.0953	0.4662	0.3381	0.1957	0.0984	0.4756	0.3664	0.2354	0.1198
	TP	0.4653	**0.3591**	**0.2182**	**0.1201**	**0.4713**	**0.3450**	**0.2186**	**0.1075**	**0.4808**	**0.3887**	**0.2467**	**0.1314**

Table 1. Detection error P_{E} of ternary SI-UNIWARD with (old) cost modulation by difference (TD) and (new) modulation by minimum perturbation (TP) with SCA-GFR / GFR feature set (whichever is better), ensemble classifier [18] and SCA-SRNet / SRNet (whichever is better).

costs. Moreover, it does not correspond to what one would intuitively expect because zero cost should be associated with $e_{ij} \approx 0$ or $|e_{ij}| \approx 1$. Additionally, precover values that are quantized to 0 experience $-1 < e_{ij} < 1$, while we require zero cost for $|e_{ij}| \approx 1$.

Computing the modulation factors as the minimum perturbation that makes the precover round to the desired stego value, for positive x_{ij}, $\rho_{ij}^{(\mathrm{TP})}(+1) = (1 - e_{ij})\rho_{ij}$ and $\rho_{ij}^{(\mathrm{TP})}(-1) = e_{ij}\rho_{ij}$, and for negative x_{ij}, $\rho_{ij}^{(\mathrm{TP})}(+1) = -e_{ij}\rho_{ij}$ and $\rho_{ij}^{(\mathrm{TP})}(-1) = (1+e_{ij})\rho_{ij}$, which can be written in a more compact form :

$$\rho_{ij}^{(\mathrm{TP})}(\mathrm{sign}(e_{ij})) = (1 - |e_{ij}|)\rho_{ij} \tag{11}$$

$$\rho_{ij}^{(\mathrm{TP})}(-\mathrm{sign}(e_{ij})) = |e_{ij}|\rho_{ij}. \tag{12}$$

For x_{ij} such that $[x_{ij}] = 0$, the minimum perturbation is different due to the character of the quantizer :

$$\rho_{ij}^{(\mathrm{TP})}(+1) = (1 - e_{ij})\rho_{ij} \tag{13}$$

$$\rho_{ij}^{(\mathrm{TP})}(-1) = (1 + e_{ij})\rho_{ij}. \tag{14}$$

Note that for $[x_{ij}] \neq 0$, the sum of both costs is equal to ρ_{ij}, while for the zero bin $\{x \in \mathbb{R} \big| [x] = 0\}$ the sum is *twice* as large: $2\rho_{ij}$. This makes intuitive sense because the quantization bin for zero coefficients is two times larger than for any other bin, and it is crucial for SI-UNIWARD to work properly in trunc JPEGs [2]. Table 2 shows the performance of (TP) modulation in trunc JPEGs.

To further validate the correctness of the (TP) cost modulation in trunc JPEGs, we compared the performance of SI-UNIWARD in regular JPEGs (with the round quantizer) embedded with payload size adjusted for constant statistical detectability according to the square root law (SRL) [16, 6, 15, 14] for a fair comparison. In particular, the relative payload in bpnzac in the round source, α_{round}, was scaled as

$$\alpha_{round} = \alpha_{trunc} \cdot \sqrt{\frac{N_{trunc}}{N_{round}}} \cdot \frac{\log(N_{round})}{\log(N_{trunc})}, \tag{15}$$

where N_{trunc} and N_{round} stand for the number of non-zero AC DCT coefficients from a given image in trunc and round JPEGs, respectively. Table 3 and Figure 3 show that even with the adjustment of the payload size according to the SRL, the (TP) cost modulation in trunc JPEGs is still more secure than in round JPEGs. This seems to indicate that the trunc source is harder to steganalyze.

Conclusions

Side-informed steganography is a term used for embedding with side-information, usually in the form of the unquantized cover called the precover. The quantization error e is used to adjust the costs of changing the cover element. In ternary schemes, this change can be either by $\mathrm{sign}(e)$ or by $-\mathrm{sign}(e)$, which can be interpreted as quantizing the precover to the second and third closest cover value, respectively. An established way to adjust the costs of both changes is to multiply the cost by $1-2|e|$ and by 1, respectively, which leads to unequal embedding change probabilities that prefer changing the cover element to the second closest value. This modulation is heuristically justified as the difference between the quantization errors to the corresponding stego and cover values.

In this work, we challenge this rule and propose modulation factors in the form of the minimal perturbation that needs to be applied to the precover to quantize to the desired stego value. Under this new rule, the modulation factor for the change by $\mathrm{sign}(e)$ (to the second closest value) stays the same, $1-2|e|$, but it becomes $1+2|e|$ when quantizing to the third closest value, i.e., by $-\mathrm{sign}(e)$. Penalizing such changes more has the biggest impact when the quantization is harsh, such as for low JPEG quality. In the spatial domain, where the quantization is fine, both rules give approximately the same performance.

For SI-UNIWARD in the JPEG domain, we observed an improvement by up to 3% in terms of P_{E} for quality 75 and the largest tested payloads (0.6 and 0.8 bpnzac). The gain generally diminishes with decreased payload and with increased JPEG quality. For quality 85 and 95, the largest gain was about 2% and 0.8%.

Our current work focuses on replacing the heuristics by deriving the embedding change rates from a precover model and the impact of embedding on the model similar to what was proposed in [5].

All code used to produce the results in this paper, including the network configuration files are available from `http://dde.binghamton.edu/download/`.

Acknowledgments

The work on this paper was supported by NSF grant No. 1561446.

References

[1] S. Agarwal and H. Farid. Photo forensics from rounding artifacts. *IEEE Transactions on Information Forensics and Security*, 2020. Under review.

[2] J. Butora and J. Fridrich. Steganography and its de-

Detector	QF 75				QF 85				QF 95			
	0.4	0.6	0.8	1	0.4	0.6	0.8	1	0.4	0.6	0.8	1
SCA-GFR	**0.4633**	**0.4256**	0.3631	0.2997	**0.4650**	**0.4147**	**0.3629**	**0.2919**	0.4868	0.4544	**0.4050**	**0.3261**
GFR	0.4686	0.4274	**0.3578**	**0.2976**	0.4735	0.4283	0.3728	0.2929	**0.4771**	**0.4524**	0.4051	0.3387
SRNet	0.4349	0.3499	0.2700	0.1908	0.4354	**0.3575**	0.2606	0.1839	**0.4561**	**0.3808**	**0.2876**	**0.1953**
SCA-SRNet	0.4349	**0.3475**	**0.2681**	**0.1840**	**0.4316**	0.3588	**0.2559**	**0.1756**	0.4569	0.3973	0.3140	0.2115

Table 2. Detection error P_{E} of ternary SI-UNIWARD with minimum perturbation (TP) in trunc JPEGs with SCA-GFR / GFR feature set, ensemble classifier and SCA-SRNet / SRNet.

JPEGs	QF 75				QF 85				QF 95			
	0.4	0.6	0.8	1	0.4	0.6	0.8	1	0.4	0.6	0.8	1
round SRL	0.4428	0.3685	0.2796	0.1932	0.4504	0.3783	0.2936	0.1931	0.4612	0.4129	0.3289	0.2238
trunc	**0.4686**	**0.4274**	**0.3578**	**0.2976**	**0.4735**	**0.4283**	**0.3728**	**0.2929**	**0.4771**	**0.4524**	**0.4051**	**0.3387**

Table 3. Detection error P_{E} of ternary SI-UNIWARD with minimum perturbation (TP) in trunc JPEGs and round JPEGs with payload scaled by SRL with GFR feature set, ensemble classifier.

tection in JPEG images obtained with the "trunc" quantizer. In *IEEE ICASSP*, Barcelona, Spain, May 4–8, 2020.

[3] T. Denemark, M. Boroumand, and J. Fridrich. Steganalysis features for content-adaptive JPEG steganography. *IEEE Transactions on Information Forensics and Security*, 11(8):1736–1746, August 2016.

[4] T. Denemark and J. Fridrich. Side-informed steganography with additive distortion. In *IEEE International Workshop on Information Forensics and Security*, Rome, Italy, November 16–19 2015.

[5] T. Denemark and J. Fridrich. Model based steganography with precover. In A. Alattar and N. D. Memon, editors, *Proceedings IS&T, Electronic Imaging, Media Watermarking, Security, and Forensics 2017*, San Francisco, CA, January 29–February 1, 2017.

[6] T. Filler, A. D. Ker, and J. Fridrich. The Square Root Law of steganographic capacity for Markov covers. In N. D. Memon, E. J. Delp, P. W. Wong, and J. Dittmann, editors, *Proceedings SPIE, Electronic Imaging, Media Forensics and Security*, volume 7254, pages 08 1–11, San Jose, CA, January 18–21, 2009.

[7] J. Fridrich and R. Du. Secure steganographic methods for palette images. In A. Pfitzmann, editor, *Information Hiding, 3rd International Workshop*, volume 1768 of Lecture Notes in Computer Science, pages 47–60, Dresden, Germany, September 29–October 1, 1999. Springer-Verlag, New York.

[8] J. Fridrich, M. Goljan, and D. Soukal. Perturbed quantization steganography using wet paper codes. In J. Dittmann and J. Fridrich, editors, *Proceedings of the 6th ACM Multimedia & Security Workshop*, pages 4–15, Magdeburg, Germany, September 20–21, 2004.

[9] J. Fridrich, M. Goljan, D. Soukal, and P. Lisoněk. Writing on wet paper. In E. J. Delp and P. W. Wong, editors, *Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VII*, volume 5681, pages 328–340, San Jose, CA, January 16–20, 2005.

[10] L. Guo, J. Ni, and Y. Q. Shi. Uniform embedding for efficient JPEG steganography. *IEEE Transactions on Information Forensics and Security*, 9(5):814–825, May 2014.

[11] V. Holub, J. Fridrich, and T. Denemark. Universal distortion design for steganography in an arbitrary domain. *EURASIP Journal on Information Security, Special Issue on Revised Selected Papers of the 1st ACM IH and MMS Workshop*, 2014:1, 2014.

[12] F. Huang, J. Huang, and Y.-Q. Shi. New channel selection rule for JPEG steganography. *IEEE Transactions on Information Forensics and Security*, 7(4):1181–1191, August 2012.

[13] A. D. Ker. A fusion of maximal likelihood and structural steganalysis. In T. Furon, F. Cayre, G. Doërr, and P. Bas, editors, *Information Hiding, 9th International Workshop*, volume 4567 of Lecture Notes in Computer Science, pages 204–219, Saint Malo, France, June 11–13, 2007. Springer-Verlag, Berlin.

[14] A. D. Ker. On the relationship between embedding costs and steganographic capacity. In M. Stamm, M. Kirchner, and S. Voloshynovskiy, editors, *The 5th ACM Workshop on Information Hiding and Multimedia Security*, Philadelphia, PA, June 20–22, 2017. ACM Press.

[15] A. D. Ker. The square root law of steganography. In M. Stamm, M. Kirchner, and S. Voloshynovskiy, editors, *The 5th ACM Workshop on Information Hiding and Multimedia Security*, Philadelphia, PA, June 20–22, 2017. ACM Press.

[16] A. D. Ker, T. Pevný, J. Kodovský, and J. Fridrich. The Square Root Law of steganographic capacity. In A. D. Ker, J. Dittmann, and J. Fridrich, editors, *Proceedings of the 10th ACM Multimedia & Security Workshop*, pages 107–116, Oxford, UK, September 22–23, 2008.

[17] Y. Kim, Z. Duric, and D. Richards. Modified matrix encoding technique for minimal distortion steganography. In J. L. Camenisch, C. S. Collberg, N. F. Johnson, and P. Sallee, editors, *Information Hiding, 8th International Workshop*, volume 4437 of Lecture Notes in Computer Science, pages 314–327, Alexandria, VA, July 10–12, 2006. Springer-Verlag, New York.

[18] J. Kodovský, J. Fridrich, and V. Holub. Ensemble classifiers for steganalysis of digital media. *IEEE Transactions on Information Forensics and Security*, 7(2):432–444, April 2012.

[19] V. Sachnev, H. J. Kim, and R. Zhang. Less detectable JPEG steganography method based on heuristic opti-

mization and BCH syndrome coding. In J. Dittmann, S. Craver, and J. Fridrich, editors, *Proceedings of the 11th ACM Multimedia & Security Workshop*, pages 131–140, Princeton, NJ, September 7–8, 2009.

[20] X. Song, F. Liu, C. Yang, X. Luo, and Y. Zhang. Steganalysis of adaptive JPEG steganography using 2D Gabor filters. In P. Comesana, J. Fridrich, and A. Alattar, editors, *3rd ACM IH&MMSec. Workshop*, Portland, Oregon, June 17–19, 2015.

[21] C. Wang and J. Ni. An efficient JPEG steganographic scheme based on the block–entropy of DCT coefficents. In *Proc. of IEEE ICASSP*, Kyoto, Japan, March 25–30, 2012.

Author Biography

Jan Butora is currently a PhD student in Electrical and Computer Engineering at Binghamton University. His research interest are in the field of media security and forensics, and, particularly steganography and steganalysis of digital images.

Jessica Fridrich is Distinguished Professor of Electrical and Computer Engineering at Binghamton University. She received her PhD in Systems Science from Binghamton University in 1995 and MS in Applied Mathematics from Czech Technical University in Prague in 1987. Her main interests are in steganography, steganalysis, and digital image forensics. Since 1995, she has received 20 research grants totaling over $11 mil that lead to more than 200 papers and 7 US patents.