Data Hiding In Images with Two JPEG of the Same Scene

[1]Trupti Bhosale, [2]Prof.V.M.Patil
Department of Computer Engineering, Zeal College of Engineering, Pune, India.

Abstract: *- It is widely known that incorporating side-information at the sender will considerably improve steganographic security in practice. Currently, most side-informed schemes utilize a top quality "precover" image that's afterwards processed so conjointly quantity and embedded with a secret. During this paper, we have a tendency to investigate another style of side-information – a group of multiple JPEG pictures of identical scene – for applications once the sender doesn't have access to a precover. The extra JPEG pictures are accustomed verify the well-liked polarity of embedding changes to modulate the prices of adjusting individual DCT coefficients in Associate in Nursing existing embedding theme. Tests on real pictures with synthesized acquisition noise and on real multiple acquisitions obtained with a tripod mounted and hand-held photographic camera show a rather important improvement in empirical security with relevance steganography utilizing one JPEG image. The projected through empirical observation determined modulation of embedding prices is even exploitation Monte Carlo simulations by showing that qualitatively identical modulation minimizes the Bhattacharyya distance between a quantity generalized Gaussian model of canopy and stego DCT coefficients corrupted by AWG acquisition noise.*

Keywords: - Steganography, side-information, precover, acquisition, security, steganalysis, JPEG;

I. INTRODUCTION

Steganography is typically cast using three characters – Alice and Bob, who communicate by hiding their messages in cover objects, and the steganalyst, the Warden, whose goal is to discover the presence of secrets. Since empirical cover sources [2], such as digital media, are too complex to be exhaustively described using tractable statistical models [3], both the steganographer and the Warden have to work with approximations. This has fundamental consequences for the steganographer[4], who is unable to achieve perfect security, as well as for the Warden, who inevitably builds sub-optimal detectors. Most consumer electronic devices, such as cell phones, tablets, and low-end digital cameras, however, save their images only in the JPEG format and thus do not give the user access to non-rounded DCT coefficients[5][6][7]. In this case, Alice can utilize a different type of side-information – she can take multiple JPEG images of the same scene. This research direction has not been developed as much mostly due to the difficulty of acquiring the required imagery and modeling the differences between acquisitions. Prior work on this topic includes where the authors made multiple scans of the same printed image on a flatbed scanner and then attempted to model the acquisition noise. Unfortunately, this requires acquiring a potentially large number of scans, which makes this approach rather labor intensive. Moreover, differences in the movement of the scanner head between individual scans lead to slight spatial misalignment that complicates using this type of side-information properly. Because this problem is especially pronounced when embedding in the pixel domain, in this paper we work with multiple images acquired in the JPEG format as we expect quantized DCT coefficients to be naturally more robust to small differences between acquisitions. Since our intention is to design a practical method, we avoid the difficult and potentially extremely time consuming task of modelling the differences between acquisitions and make the approach work well even when mere two images are available to Alice. In another relevant prior art, the authors proposed embedding by stitching patches from multiple acquisitions in a predefined pattern. The individual patches are not modified and are therefore statistically indistinguishable from the original images. However, as the authors discussed in their paper there are likely going to be detectable differences between individual patches and inconsistencies at their boundaries.

Furthermore, the required number of acquisitions quickly grows with the length of the secret message. By using 150 acquisitions of the same scene (scans), the authors were able to embed only 0.157 bits per non-zero AC coefficient on average. We first report the results of experiments on BURSTbase for J-UNIWARD costs [8] across a wide range of quality factors and payloads and contrasted with J-UNIWARD and SI-UNIWARD to see the gain w.r.t. using only a single JPEG image and the comparison to other type of side-information. We also investigate how the gain in security decreases with increased differences between exposures. This section continues with a summary of experiments on BURSTbaseH images with hand-held camera on both J-UNIWARD and UED-JC[9]. Although the security gain is smaller than for BURSTbase, when the steganographer rejects bad bursts, a significant security gain is still observed w.r.t. steganography with a single JPEG. Finally, the appendix contains analysis that explains the shape of the experimentally determined modulation of costs.

II. LITERATURE SURVEY

E. Franz and A. Schneidewind, E. Franz,K. Petrowski [12], [13], [14]authors made multiple scans of the same printed image on a flatbed scanner and then attempted to model the acquisition noise. Unfortunately, this requires acquiring a potentially large number of scans, which makes this approach rather labor intensive.

T. Denemark and J. Fridrich, [15] authors proposed embedding by stitching patches from multiple acquisitions in a predefined pattern. The individual patches are not modified and are therefore statistically indistinguishable from the original images.

A. Foi, M. Trimeche, V. Katkovnik, and K. Egiazarian [17] authors proposed Images acquired using an imaging sensor are noisy measurements of the true scener by which we understand the image rendered by the camera lens. The randomness in the form of noise or imperfections is introduced by several separate mechanisms

E. Franz, [11], a ternary version of SI-UNIWARD was studied where the authors argued that, as the rounding error eij becomes small, the embedding rule should be allowed to change the coefficient both ways.

V. Holub, J. Fridrich, and T. Denemark [9] authors proposed The GFR features were selected for the design because they are known to be highly effective against modern JPEG steganography, including J-UNIWARD and all versions of UED . Y. Kim, Z. Duric, and D. Richards, V. Sachnev, H. J. Kim, and R. Zhang,F. Huang, J. Huang, and Y.-Q. Shi,L. Guo, J. Ni, and Y. Q. Shi [5], [6], [7], [8], [9], [10], [11]authors proposed which embeds secrets when converting a true-color image to a palette format. By far the most common side-informed steganography today hides in JPEG images using non-rounded DCT coefficients

J. Fridrich, M. Goljan, and D. Soukal, [4]authors proposed embed her secret while processing the precover and/or converting it to a different format. The first example of this technique is the embedding-whiledithering steganography.

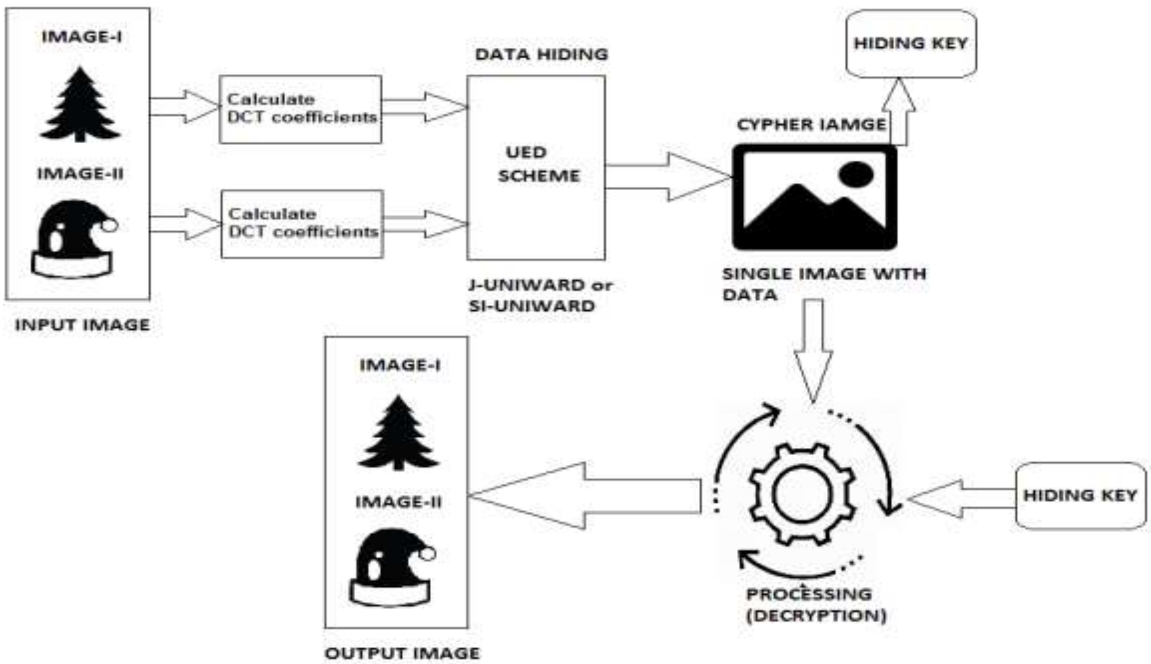

Figure 1: Architecture Diagram

III. PROPOSED SYSTEM AND ALGORITHMS

This manuscript is an expanded version of an abbreviated version of this work published at IEEE ICASSP. In particular, this 13-page manuscript extends the page conference paper in the following important aspects:

- The proposed method is introduced in a more general setting applicable to any cost-based embedding scheme operating in the JPEG domain. Likewise, it is implemented and tested for other embedding schemes besides J-UNIWARD, such as the UED-JC steganography.
- The qualitative dependence of the modulation factor for adjusting the costs of DCT coefficients on the JPEG quality factor is explained with Monte Carlo simulations by employing a generalized Gaussian model of DCT coefficients.
- The database used in the main bulk of experiments, the BURSTbase, is analysed in detail to put forward evidence that the two closest images from BURSTbase indeed differ primarily in the acquisition noise with heteroscedastic properties.
- The experimental section was substantially expanded with a) experiments on images taken with a hand-held camera to show the practicality of the proposed method, b) experiments on simulated acquisition noise to show that in this ideal case the proposed method can outperform even side-informed steganography with a single high-quality precover (this gain is explained by contrasting steganography with precover and with two JPEGs w.r.t. the number of correctly and incorrectly determined directions of changes to be modulated), c) experiments on the UED-JC embedding algorithm to show the generality of the proposed methodology, and d) experiments showing that by rejecting bad bursts the steganographer can retain a rather significant advantage of embedding with two JPEGs w.r.t. a single JPEG.
- Specific ideas for technology transfer of the proposed method are put forward.

Algorithm 1 Pseudo-code for side-informed embedding with two JPEGs.

Input: Two quality factor Q JPEG images with quantized DCT coefficients $x_{ij}^{(1)}$ and $x_{ij}^{(1)}$, $1 \leq i \leq M$, $1 \leq j \leq N$
Output: Stego JPEG image with DCT coefficients $y_{ij}^{(1)}$
Compute costs $\rho_{ij}^{(0)}(-1), \rho_{ij}^{(0)}(+1)$ of DCT coefficients from JPEG $x_{ij}^{(1)}$ (the cover)
for $i = 1, \ldots, M$ **do**
  for $j = 1, \ldots, N$ **do**
    $\rho_{ij}(\pm 1) = \rho_{ij}^{(0)}(\pm 1)$
    $s_{ij} = \text{sign}(x_{ij}^{(2)} - x_{ij}^{(1)})$
    IF $x_{ij}^{(1)} \neq x_{ij}^{(2)}$ THEN $\rho_{ij}(s_{ij}) = m(Q)\rho_{ij}^{(0)}(s_{ij})$
  end for
end for
Embed message in $x_{ij}^{(1)}$ using costs ρ_{ij} using STCs to obtain stego JPEG file with DCT coefficients y_{ij}
Recipient reads the secret message using STCs from the stego JPEG file y_{ij}

IV. CONCLUSION

We study steganography with side-information at the sender in the form of a second JPEG image of the same scene that is used to infer the preferred direction of steganography embedding changes. This information is incorporated into the embedding algorithm by decreasing (modulating) the embedding costs of such preferred changes. Experiments with real multiple acquisitions show a quite significant increase in empirical security of with respect to steganography with a single cover image (J-UNIWARD). The boost in empirical security appears fairly insensitive to small differences between the two acquisitions, which makes the proposed method practical and opens up the possibility to use multiple exposures obtained using a hand-held camera or acquiring multiple exposures from short video clips.

REFERENCES

[1] Tomáš Denemark, *Steganography with Multiple JPEG Images of the Same Scene*. DOI 10.1109/TIFS.2017.2705625, IEEE Transactions on Information Forensics and Security Page(s): 2308 - 2319 May 2017

[2] R. Böhme, Advanced Statistical Steganalysis, Springer-Verlag, Berlin Heidelberg, 2010.

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

[4] J. Fridrich and R. Du, “Secure steganographic methods for palette images,” in Information Hiding, 3rd International Workshop, A. Pfitzmann, Ed., Dresden, Germany, September 29–October 1, 1999, vol. 1768 of Lecture Notes in Computer Science, pp. 47–60, Springer-Verlag, New York.

[5] J. Fridrich, M. Goljan, and D. Soukal, “Perturbed quantization steganography using wet paper codes,” in Proceedings of the 6th ACM Multimedia & Security Workshop, J. Dittmann and J. Fridrich, Eds., Magdeburg, Germany, September 20–21, 2004,pp. 4–15.

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

[7] V. Sachnev, H. J. Kim, and R. Zhang, “Less detectable JPEG steganography method based on heuristic optimization and BCH syndrome coding,” in Proceedings of the 11th ACM Multimedia & Security Workshop, J. Dittmann, S. Craver, and J. Fridrich, Eds., Princeton, NJ, September 7–8, 2009, pp. 131–140.

[8] F. Huang, J. Huang, and Y.-Q. Shi, “New channel selection rule for JPEG steganography,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 4, pp. 1181–1191, August2012.

[9] L. Guo, J. Ni, and Y. Q. Shi, “Uniform embedding for efficient JPEG steganography,” IEEE Transactions on Information Forensics and Security, vol. 9, no. 5, pp. 814–825, May 2014.

[10] 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, vol. 2014:1, 2014.

[11] E. Franz, “Steganography preserving statistical properties,” in Information Hiding, 5th International Workshop, F. A. P. Petitcolas, Ed., Noordwijkerhout, The Netherlands, October 7– 9, 2002, vol. 2578 of Lecture Notes in Computer Science, pp. 278–294, Springer-Verlag, New York.

[12] E. Franz and A. Schneidewind, “Pre-processing for adding noise steganography,” in Information Hiding, 7th International Workshop, M. Barni, J. Herrera, S. Katzenbeisser, and F. Pérez- González, Eds., Barcelona, Spain, June 6–8, 2005, vol. 3727 of Lecture Notes in Computer Science, pp. 189–203, Springer- Verlag, Berlin.

[13] E. Franz, “Embedding considering dependencies between pixels,”
in Proceedings SPIE, Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, E. J. Delp, P. W. Wong, J. Dittmann, and N. D. Memon, Eds., San Jose, CA, January 27–31, 2008, vol. 6819, pp. D 1– 12.

[14] K. Petrowski, M. Kharrazi, H. T. Sencar, and N. Memon, “PSTEG: steganographic embedding through patching [image steganography],” in Proc. IEEE ICASSP, Philadelphia, PA, March 18–23, 2005.

[15] T. Denemark and J. Fridrich, “Side-informed steganography with two JPEGs,” in Proc. IEEE ICASSP, New Orleans, LA, March 5–8, 2017.

[16] A. Foi, M. Trimeche, V. Katkovnik, and K. Egiazarian, “Practical
Poissonian-Gaussian noise modeling and fitting for singleimage raw-data,” IEEE Transactions on Image Processing, vol. 17, no. 10, pp. 1737–1754, October 2008.