Final Report

- Grant/Contract Title: Adaptive Steganography
- Grant/Contract Number: FA9550- 07-1-0017
- Principal Investigator: Gaurav Sharma
- Date: March 28, 2011

Abstract

The research conducted under this grant has addressed the area of Adaptive Steganography, covering the domains of data hiding, data embedding, and forensics. Key accomplishments include the development of an entirely new and novel framework for data hiding using a set theoretic feasibility and optimization framework, forensic analyses encompassing both device/print forensics, extensions to media security and hardcopy data encoding. Of these accomplishments, the new framework for data hiding using a set theoretic feasibility framework represents a major advance in the field of data hiding that has led to the development of a new conceptual framework for data hiding based on signal processing considerations as opposed to the commonly accepted communications framework. The communications framework considers the data hiding problem purely from a communications perspective and uses ad hoc modifications to incorporate the perceptual signal processing constraints, which are not integral to the framework. The versatility of this framework has been demonstrated through its applications in data hiding, steganography, and fingerprinting. The framework encompasses both spread spectrum and Quantization Index Modulation (QIM) watermarking methods and also enables extensions to optimality where one criterion is optimized while maintaining other constraints. The overall work has resulted in ten journal and conference publications.

Major Accomplishment: Set-Theoretic Framework For Data Hiding [4,6,7-10]

Conventionally, data hiding has been considered as a communications problem, with or without side-information. Our work in this area considers data hiding from an entirely new perspective as a signal feasibility problem. The message detectability and perceptual transparency are posed as constraints on the cover signal and the objective of data hiding is to meet these constraints along with other application dependent constraints. The watermark detectability constraints can comprehend both spread spectrum and QIM watermarks. Additional optional constraints address robustness to compression, statistical indistinguishability, robustness against collusion, and fragility under aggressive modification. A number of these constraint sets are shown to be convex and convex approximations are demonstrated for others, enabling solution of the set theoretic watermarking feasibility problem in a computationally efficient manner by the method of projections onto convex sets. The formulation elegantly handles multiple watermarks and arbitrary transform domain watermarks and compression.

A conceptual representation of the methodology is shown in Fig. 1, where the common constraints in watermarking are shown as two-dimensional convex constraint set. The sequence of projections f_1, $f_{2, \ldots}$ f_4 illustrates a sample sequence obtained via the method of projections on to convex sets which converges to a point that meets all the constraints. The extension of the methodology to optimal embedding is illustrated in Fig. 2, where two constraint sets S_1 and S_2 and level set boundaries corresponding to the optimization function values of u_i and l_i are shown along with a test value t_i which is midway between these. The problem is feasible when the objective function is replaced by a constraint that places an upper bound constraint of u_i on the objective function and infeasible for an upper bound of l_i. At each step, the feasibility is tested for the value t_i located midway between l_i and u_i and if the problem is feasible u_i is replaced by t_i, otherwise l_i is replaced by t_i. This bisection process rapidly converges to the optimal point.

Figure 3, illustrates a set of optimal images obtained using the proposed method according to different optimality criteria indicated below the images and Figure 4, indicates the corresponding watermark signal images and Fig 5. their Fourier spectra.The utility of the framework is apparent in these images the embedded watermark signals implicitly adapt to the cover image so as to meet the constraints. The different objectives of the different constraints are also apparent in the different optimal images.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
28 MAR 2011		**01-12-2006 to 30-09-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Adaptive Steganography	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **University of Rochester,Strong Memorial Hospital,601 Elmwood Ave,Rochester,NY, 14642-**	8. PERFORMING ORGANIZATION REPORT NUMBER **; AFRL-OSR-VA-TR-11-060**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S) **AFRL-OSR-VA-TR-11-060**

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The research conducted under this grant has addressed the area of Adaptive Steganography, covering the domains of data hiding, data embedding, and forensics. Key accomplishments include the development of an entirely new and novel framework for data hiding using a set theoretic feasibility and optimization framework, forensic analyses encompassing both device/print forensics, extensions to media security and hardcopy data encoding. Of these accomplishments, the new framework for data hiding using a set theoretic feasibility framework represents a major advance in the field of data hiding that has led to the development of a new conceptual framework for data hiding based on signal processing considerations as opposed to the commonly accepted communications framework. The communications framework considers the data hiding problem purely from a communications perspective and uses ad hoc modifications to incorporate the perceptual signal processing constraints, which are not integral to the framework. The versatility of this framework has been demonstrated through its applications in data hiding, steganography, and fingerprinting. The framework encompasses both spread spectrum and Quantization Index Modulation (QIM)watermarking methods and also enables extensions to optimality where one criterion is optimized while maintaining other constraints. The overall work has resulted in ten journal and conference publications.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**6**	

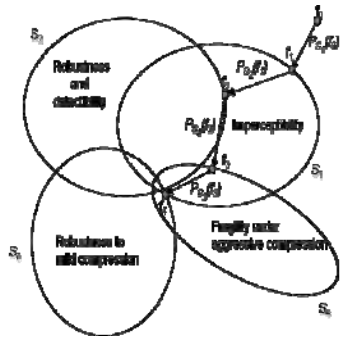

Fig 1: Watermarking by Projections on to Convex Sets

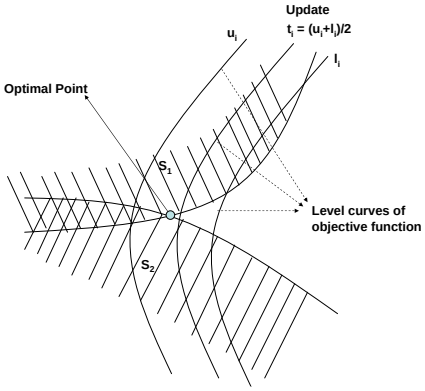

Fig 2: Bisection search for optimality via feasibility

Fig. 3. Watermarked versions of the Boat image obtained for the four different optimization formulations. (a) Maximizing embedding strength. PSWR of the image is 24.60 dB. (b) Minimizing frequency weighted perceptual distortion. PSWR of the image is 37.71 dB. (c) Maximizing robustness to compression. PSWR of the image is 24.79 dB. (d) Minimizing the watermark texture visibility. PSWR of the image is 37.28 dB.

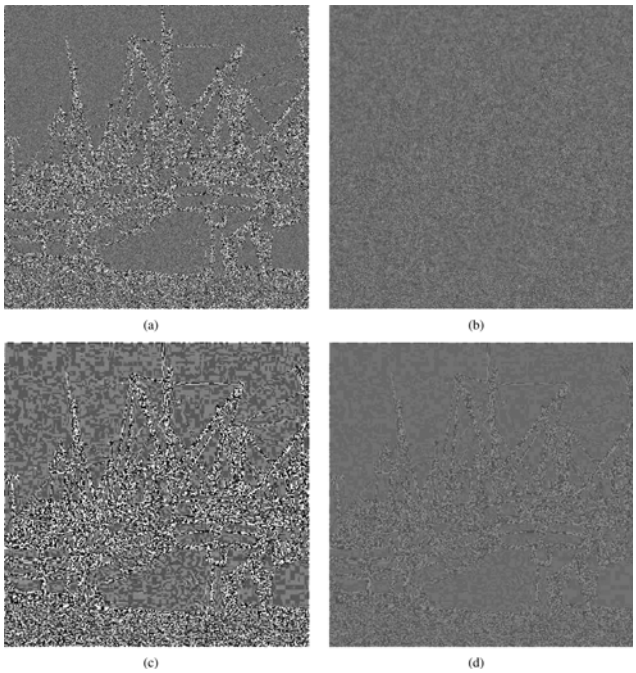

Fig. 4. Embedded watermark signals corresponding to the difference between the watermarked Boat image and the original Boat image for the four different optimization formulations. (a) Maximizing embedding strength. (b) Minimizing frequency weighted perceptual distortion. (c) Maximizing robustness to compression. (d) Minimizing the watermark texture visibility. Values have been scaled by a factor of 4 and translated to a mid gray value of 128 to make differences clearer and to allow representation of both positive and negative values.

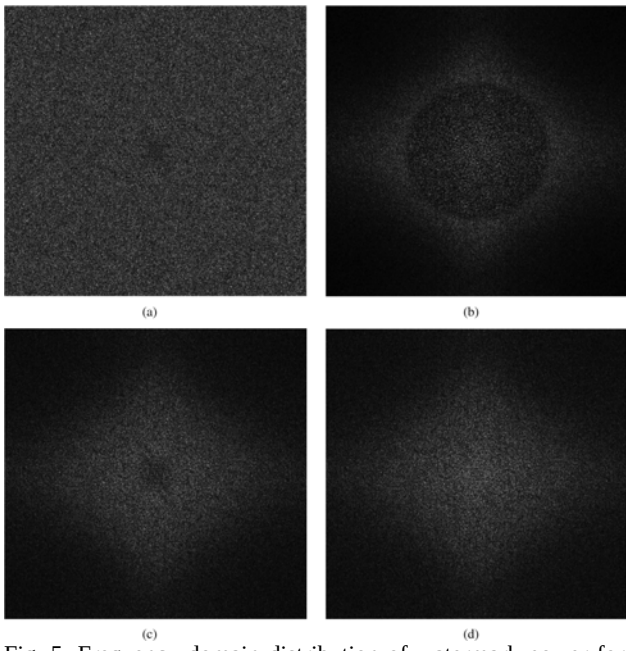

Fig. 5. Frequency domain distribution of watermark power for the optimally watermarked Boat images. The figures represent the magnitudes of the embedded watermark signals for the four different optimization formulations. (a) Maximizing embedding strength. (b) Minimizing frequency weighted perceptual distortion. (c) Maximizing robustness to compression. (d) Minimizing the watermark texture visibility.

Other Accomplishments:

Other work in this project has addressed a number of new avenues in steganography, data hiding, data embedding and forensics. Specifically, in the forensics area we have posed the problem of temporal forensics and proposed an information theoretic framework for temporal ordering of forensic signatures using the data processing inequality [3].In addition, we have extensively investigated the forensic detection of seam-carving, the leading method for content adaptive re-targeting of image data [2] and hardcopy image barcodes for exploring the tradeoff between image quality and data robustness in printed documents. We have also addressed device forensics for printers using geometric distortion signatures [5] and proposed and analyzed a robust media encryption technique based on compressed sensing. Details of these accomplishments can be found in the cited publications which are available a the PIs website.

Impact on the Community

The research conducted under this grant has had a remarkable impact in the community.

1) As already noted, it has led to the development of an entirely new way of thinking about data hiding that incorporates perceptual constraints holistically in the problem formulation instead of requiring these to be added in after the fact as ad hoc modifications **[4,6,7-10]**. The method also comprehends multiple watermarks in an integrated and principled fashion and offers a flexible framework in which constraints can be added or dropped depending on the application requirements.
2) Additional outgrowths of the research have led to:
    a. Methods for robust media encryption based on compressed sensing and a preliminary security analysis of these methods [6]
    b. An empirical game theoretic formulation of steganography when the steganographer and steganalyst operate under limited resource constraints [8].
    c. Forensic methods for detecting seam carving, the most prominent method for content adaptive scaling of images [2].
    d. Hardcopy forensics based on geometric distortion signatures [5] and a novel new problem of temporal forensics with an information theoretic approach for temporal ordering [3].

Current Year Transition Information

In the current year, the project work was conducted under a no cost extension that was necessitated by the departure of some of the students on the grant. Adem Orsdemir left to pursue a PhD in Business and Junwen Mao left after completing her MS. Oktay Altun defended his PhD thesis.The work was transitioned from Oktay Altun, Adem Orsdemir, and Junwen Mao to Orhan Bulan and the PI.

1. O. Bulan and G. Sharma, “High capacity image barcodes using color separability,” in Proc. SPIE: Color Imaging XVI: Displaying, Processing, Hardcopy, and Applications, vol. 7866, 24-27 January 2011, San Jose, CA, USA, pp. 7866-22,1-9.
2. C. Fillion and G. Sharma, “Detecting content adaptive scaling of images for forensic applications,” in Proc. SPIE: Media Forensics and Security XII, vol. 7541, 17-21 January 2010, San Jose, CA, USA, pp. 7541--36.
3. J. Mao, O. Bulan, G. Sharma, and S. Datta , “ Device temporal forensics: An information theoretic approach,” in Proc. IEEE Intl. Conf. Image Proc., 7-11 November 2009, Cairo, Egypt, pp 1501--1503.
4. H. O. Altun, A. Orsdemir, G. Sharma, and M. F. Bocko, “Optimal Spread Spectrum Watermark Embedding via a Multistep Feasibility Formulation,” IEEE Trans. Image Proc., vol. 18, no. 2, Feb. 2009, pp. 371–387.
5. O. Bulan, J. Mao, and G. Sharma, “Geometric distortion signatures for printer identification,” in Proc. IEEE Intl. Conf. Acoustics Speech and Sig. Proc., Taipei, Taiwan, 20-24 Apr. 2009, pp. 1401-1404.
6. A. Orsdemir, H. Oktay Altun, G. Sharma, and M. F. Bocko, “On the security and robustness of encryption via compressed sensing,” in Proceedings Military Communications Conference (MILCOM), Nov. 17-19, 2008, San Diego, CA, [CDROM].
7. O. Altun, O. Bulan, G. Sharma, and M. Bocko, “Improved embedding efficiency and AWGN robustness for SS watermarks via pre-coding,” In Delp et al. Proc. SPIE: Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, vol. 6819, Jan. 2008, San Jose, CA, pp. 68191F-1–12.

8. A. Orsdemir, O. Altun, G. Sharma, and M. Bocko, “Steganalysis-aware Steganography: Statistical indistinguishability despite high distortion,” In Delp et al. Proc. SPIE: Security, Forensics, Steganography, and Watermarking of Multimedia Contents X , vol. 6819, Jan. 2008, San Jose, CA, pp. 681915–1–9.
9. O. Altun, G. Sharma, A. Orsdemir, and M. Bocko, “ Collusion resilient fingerprint design by alternating projections,” in Proc. IEEE Intl. Conf. Image Proc., 16-19 Sept. 2007, San Antonio, TX, vol. IV, pp. 437--440.
10. O. Altun, G. Sharma, M. U. Celik, M. Bocko, "A set theoretic framework for watermarking and its application to semifragile tamper detection," IEEE Trans. Info. Forensics and Security, vol. 1, no. 4, Dec. 2006, pp. 479--492.