Chapter 6
An Adaptive JPEG Steganographic Scheme Based on the Block Entropy of DCT Coefficients

Chang Wang
Sun Yat-sen University, China

Chuntao Wang
South China Agricultural University, China

Jiangqun Ni
Sun Yat-sen University, China

Ruiyu Zhang
Sun Yat-sen University, China

ABSTRACT

Minimizing the embedding impact is a practically feasible philosophy in designing steganographic systems. The development of steganographic systems can be formulated as the construction of distortion profile reflecting the embedding impact and the design of syndrome coding based on a certain code. The authors devise a new distortion profile exploring both the block complexity and the distortion effect due to flipping and rounding errors, and incorporate it in the framework of syndrome trellis coding (STC) to propose a new JPEG steganographic scheme. The STC provides multiple candidate solutions to embed messages to a block of coefficients while the constructed content-adaptive distortion profile guides the determination of the best solution with minimal distortion effect. The total embedding distortion or impact would be significantly reduced and lead to the less detectability of steganalysis. Extensive experimental results demonstrate that the proposed JPEG steganographic scheme greatly increases the secure embedding capacity against steganalysis and shows significant superiority over some existing JPEG steganographic approaches.

DOI: 10.4018/978-1-4666-4006-1.ch006

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

Steganography is the art of covert communication, in which secret messages are embedded into the digital medias, e.g., audio, video and image. In more detail, steganographic systems slightly modify cover works to hide the message and yield stego works accordingly, where a key shared by the sender and receiver is usually adopted to enhance the security. The major objective of steganographic systems is the statistical undetectability against steganalysis, i.e., the existence of hidden message in stego works cannot be detected via statistical methods (Filler, Judas, & Fridrich, 2010; Cox, Miller, Bloom, & Fridrich, 2008). In practice, the statistical undetectability is usually evaluated by applying some state-of-the-art steganalysis tools to check if the stego and cover works in the test set can be correctly classified.

The past decades have witnessed the rapid development of steganographic algorithms and practical systems, especially for digital images For instance, one of the most popular steganographic approaches for digital images is the least significant bit (LSB) replacement (Peticolas, Anderson, & Kuhn, 1999) and its variants (Zhang, Wang, & Zhang, 1998; Sharp, 2001; Provos, 2001) (see also the references therein). These earlier methods can be easily detected via statistical analysis.

Since the JPEG format is the widely-adopted format for image storage and transmission, JPEG steganography has become the domain of extensive research. In the literatures, a number of different schemes have been developed for JPEG steganography, such as Jsteg (Upham, 1997), Outguess (Provos, 1999), the model-based steganography (MB) (Sallee, 2003), F5 (Westfeld, 2001), etc.

Historically, Jsteg is one of the first steganographic schemes for JPEG image, which embeds the given message bits by substituting the LSBs of quantized discrete cosine transform (DCT) coefficients. Jsteg, however, can be easily detected by common steganalysis tools, such as PEV274 (Pevny & Fridrich, 2007), due to the histogram abnormality of DCT coefficients introduced in embedding. In contrast to Jsteg, Outguess was proposed to preserve the histogram shape of quantized DCT coefficients after embedding. It consists of two stages, i.e., in stage-1, it selects the DCT coefficients with non-zero and non-unity magnitude and then embeds the message bits in a pseudo-random way into the chosen coefficients, while in stage-2, it corrects the magnitude of some DCT coefficients to preserve the original histogram. Another scheme following the similar spirit is MB. It employs the generalized Cauchy distribution to model the DCT coefficients and designs the embedding rule to preserve the original Cauchy distribution as much as possible. MB achieves relatively high embedding capacity while preserving the employed model.

F5 is one of the most popular steganographic schemes for JPEG steganography. It improves F3 and F4, and achieves an embedding rate with less steganographic changes (Westfeld, 2001). F5 adopts the techniques of straddling and matrix encoding to enhance the undetectability against steganalysis. The straddling mechanism utilizes permutation to shuffle the coefficients to make the modifications uniformly distributed over the whole image, while the matrix encoding (also known as *syndrome coding*) increases the embedding efficiency, i.e., the number of inserted bits per unit distortion. Thanks to the gain in embedding efficiency, a lot of steganographic schemes based on matrix encoding hereafter have been proposed in the literatures (Kim, Duric, & Rechards, 2007; Fridich & Soukual, 2006; Choi & Kim, 2009; Zhang & Wang, 2009; Fridrich, Pevny, & Kodavsky, 2007; Bierbrauer & Fridrich, 2008).

In the past few years, another principle aiming to minimize the embedding impact in steganography has aroused great interests (Fridrich, 2006; Cox, Miller, Bloom, & Fridrich, 2008; Fridrich, Pevny, & Kodavsky, 2007). In the framework of minimizing the embedding impact, each coefficient is assigned with a weight indicating the contribution of making change at that coefficient

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/adaptive-jpeg-steganographic-scheme-based/75665

Related Content

Surveillance in Public Spaces as a Means of Protecting Security: Questions of Legitimacy and Policy
Anna Tsiftsoglou (2012). *Cyber Crime: Concepts, Methodologies, Tools and Applications (pp. 300-309).*
www.irma-international.org/chapter/surveillance-public-spaces-means-protecting/60955

Consumer Risk Perception Towards Cybercrimes and E-Commerce: The Case of Malaysia
Hui Nee Au Yong, Yoke Chin Kuah, Chooi Yi Weiand Abdul Rafay (2023). *Theory and Practice of Illegitimate Finance (pp. 184-202).*
www.irma-international.org/chapter/consumer-risk-perception-towards-cybercrimes-and-e-commerce/330632

A Cyber Crime Investigation Model Based on Case Characteristics
Zhi Jun Liu (2017). *International Journal of Digital Crime and Forensics (pp. 40-47).*
www.irma-international.org/article/a-cyber-crime-investigation-model-based-on-case-characteristics/188361

Monitor and Detect Suspicious Transactions With Database Forensic Analysis
Harmeet Kaur Khanujaand Dattatraya Adane (2020). *Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice (pp. 402-426).*
www.irma-international.org/chapter/monitor-and-detect-suspicious-transactions-with-database-forensic-analysis/252703

Effective Security Assessments and Testing
David Culbreth, Adan Guadarramaand Ayad Barsoum (2020). *International Journal of Cyber Research and Education (pp. 17-23).*
www.irma-international.org/article/effective-security-assessments-and-testing/258289