Computational Intelligence in Steganalysis Environment

ROSHIDI DIN, AZMAN SAMSUDIN
School of Computer Sciences
Universiti Sains Malaysia (USM)
Minden, Pulau Pinang,
MALAYSIA

roshidi@uum.edu.my, azman@cs.usm.my http://www.cs.usm.my

Abstract: - This paper presents gives a consolidated view of digital media steganalysis from the perspective of computational intelligence (CI). The environment of digital media steganalysis can be divided into three (3) domains which are image steganalysis, audio steganalysis, and video steganalysis. Three (3) major methods have also been identified in the computational intelligence based on these steganalysis domains which are bayesian, neural network, and genetic algorithm. Each of these methods has pros and cons. Therefore, it depends on the steganalyst to use and choose a suitable method based on their purposes and its environment.

Key-Words: - Steganalysis, Computational Intelligence, Image, Audio, Video

1 Introduction

Over the last decade, one of the most significant current discussions in legal and computer science is the field of information security. One of the concerns in the area of information security is the concept of hidden-information or information hiding. There are two main purposes in information hiding: (1) to protect against the detection of secret messages by a passive adversary, and (2) to hide data so that even an active adversary cannot remove the data. Most of the proposed information hiding system is designed based on steganography. Steganography is a method that uses a covert communication between two parties whose existence is unknown to a possible attacker. That is highly over claim statement that steganography can play an important role in protecting the security of highly sensitive documents over the Internet in this era of terabit networks.

Many of the new directions in steganography came from attack analyses. This process of analyzing steganographic protocols is carried out in order to detect and extract secret messages. This is called steganalysis which is generally starts with several suspected information streams but uncertain whether any of information stream contains hidden messages. Hence, steganalysis is the process of detecting steganography by looking at variances between bit patterns and unusually large file sizes. It is the art of discovering and rendering hidden data from useless covert messages. Several studies suggest that to have a good steganalysis tool, the implementation of steganalysis system should involve some degree of computational intelligence (CI). One of a few of such analysis [1] found that a supervised learning based approach using CI can be implemented to solve steganalysis problem. Thus, the purpose of this paper is to discuss the implementation of CI methods on steganalysis task. Several domain area of steganalysis environment has been formalized in order to justify each domain area against the right CI methods.

2 Artificial Intelligence

Artificial intelligence (AI) is both an art and a science [2]. Generally speaking, AI systems are built around into two types of automated inference reasoning engines which are forward reasoning and backwards reasoning. Meanwhile, AI applications can be also divided into two types, in terms of consequences: classifiers ("if pretty then flower") and controllers ("if pretty then take it"). Controllers do however classify conditions before inferring actions, and therefore classification forms a central part of most AI systems. The ultimate achievement in this field would be to develop a tool that can replicate or exceed human internal capabilities, including reasoning, recognition, understanding, imagination, creativity, and emotions. Due to that, the development of several useful computing tools has arisen in order to achieve these ideas in AI field. The tools of particular interest can be roughly divided into conventional AI, computational intelligence, and hybrid systems as shown in Fig.1.

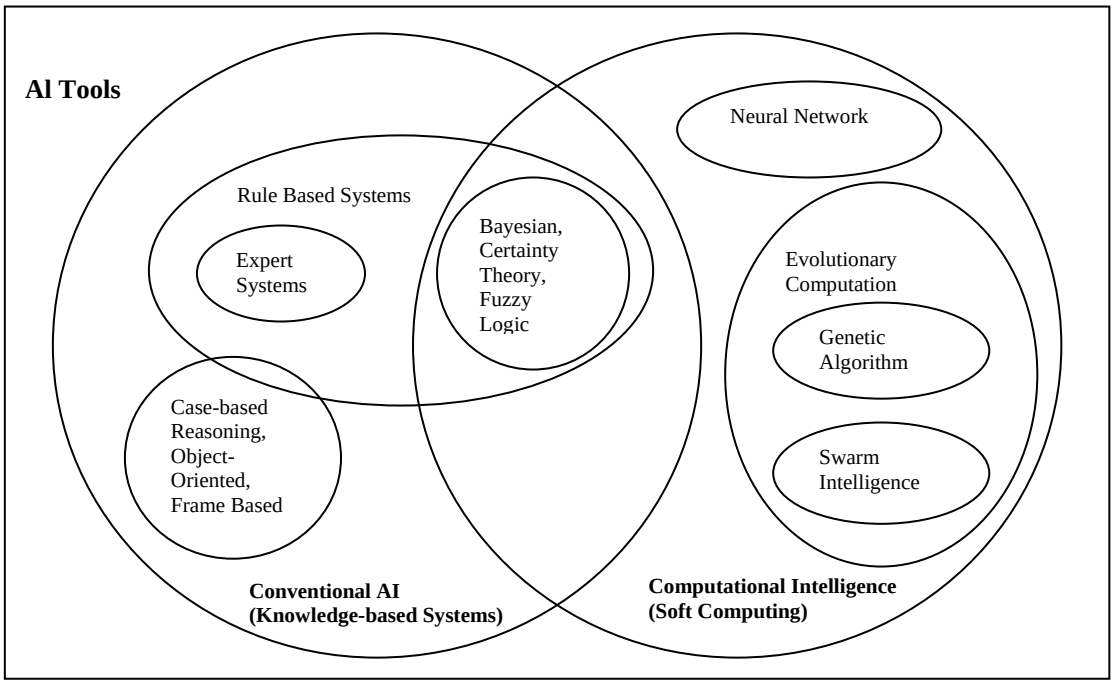

Fig.1 Categories of computing tools (adapted from [3, 4])

2.1 Convention AI

Conventional AI which is also known as knowledge based systems is being applied in many of the traditional rule-based AI areas. Researchers are trying to develop AI systems that are capable of performing in a limited sense, "like a human being" [5]. Knowledge based systems include expert system and rule based systems, object-oriented and frame based systems, and intelligent agents. Mostly conventional AI can be classified as machine learning, characterized by formalism and statistical analysis. This is also known as symbolic AI, logical AI, neat AI and Good Old Fashioned Artificial Intelligence (GOFAI).

2.2 Computation Intelligence (CI)

CI is a very young discipline and other disciplines such as philosophy, neurobiology, evolutionary biology, and psychology have been studying intelligence much longer. Computational intelligence (CI) is the study of the design of intelligent agents which involves iterative development or learning. Computational intelligence includes neural networks, evolutionary computation (genetic algorithms and swarm intelligence) and other optimization algorithms. Techniques for handling uncertainty, such as bayesian, fuzzy logic, certainty theory fit into both categories. All these techniques use a mixture of rules and associated numerical values.

Currently, subjects in computational intelligence as defined by IEEE Computational Intelligence Society includes fuzzy systems, neural networks and evolutionary computation (genetic algorithms and swarm intelligence).

2.3 Hybrid System

With hybrid intelligent system, attempts are made to combine at least two CI disciplines. There are several ways in which different computational techniques can be complementary as hybrid intelligent system which are including dealing with multifaceted problems, capability enhancement, parameter setting and clarification and verification.

3 Computational Intelligence on Steganalysis

Commonly, the implementation of computational intelligence, and their hybrids methods in steganalysis environment are collectively referred to as *intelligent steganalytic systems* (ISS) shown in Fig.2. This figure represents a steganalysis environment which is an intelligent synthesis from bayesian, neural network, fuzzy system and genetic algorithm methods.

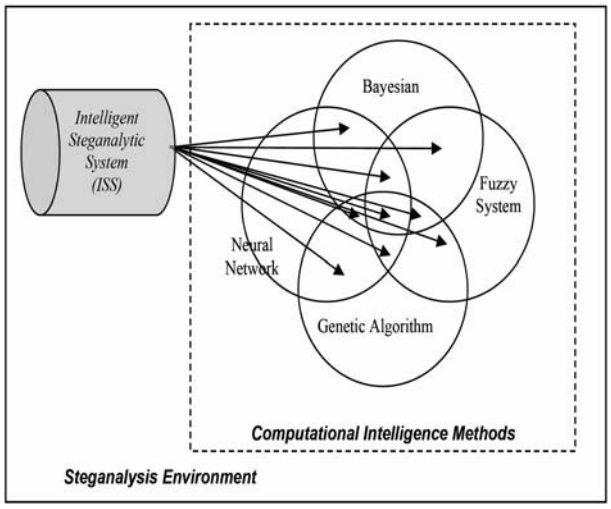

Fig.2 Synthesis of CI methods on steganalysis environment (adopted from [6])

- Generally, ISS involve two, three or more of these CI methods that are either used in series or integrated in a way to produce advantageous results through synergistic interactions [7]. It is important when considering the varied nature of application domains. There are three (3) main reasons for creating ISS which are technique enhancement, multiplicity of application task and realizing multi-functionality [8].

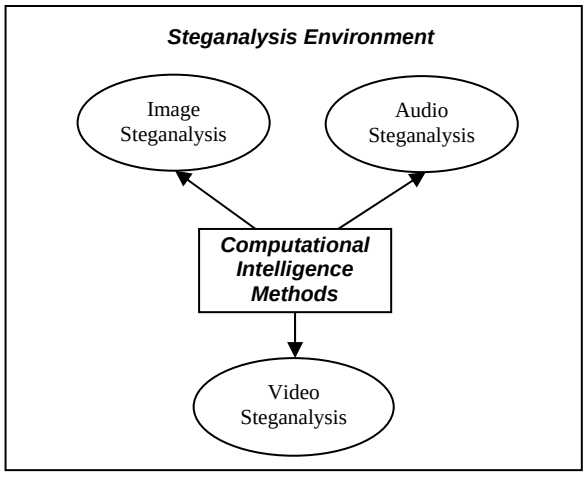

Fig.3 Computational intelligence on steganalysis domain in digital medium

Nowadays, many researchers have applying CI on steganalysis environment. Most of their results have proven that the application of CI methods has given a great influence on steganalysis performance. They have also identified that the steganalysis environment can be divided into three (3) domains which are image steganalysis, audio steganalysis, and video steganalysis as shown in Fig.3. Despite different computational intelligence based approaches been proposed, the possibilities of using the techniques for steganalysis are still under-utilized.

3.1 Image Steganalysis

Currently, several methods for detecting image steganography with CI such as LSB embedding [9], spread spectrum steganography [10], and LSB matching [11, 12], have been successfully steganalyzed [13].

a) Bayesian: On analyzing an image, one steganalysis approach [14] had proposed to estimate the hidden message based on a Bayesian framework. Message embedding in bit planes of an image is modeled as a binary symmetric channel. However, this method does not work for LSB embedding due to the lack of statistical structure in the bit plane.

b) Neural Network: A neural network [15] has been applied to analyze the possible occurrences of certain image pattern through histogram to detect the presence of data. They have used neural network approach to check for those discrepancy patterns and trains itself for better accuracy by automating the whole process from decomposition, signature searching, detection and elimination of the detection framework. In another study, method based on neural network [16] has proposed to gather statistics features of images to identify the underlying hidden data. This study used neural network to analyze object digital image based on three different types of transformation which are Domain Frequency Transform (DFT), Domain Coefficient Transform (DCT) and Domain Wavelet Transform (DWT). Meanwhile, the work of detection of wavelet domain information hiding techniques [17] has suggested statistical analysis on the texture of an image. Wavelet coefficients in each sub-band of wavelet transform are modeled as a Generalized Gaussian distribution (GGD) with two parameters. It appears that those parameters are a good measure of image features and can be used to discriminate stego-images from innocent images. Neural network is adopted to train these parameters to get the inherent characteristic of innocent and stego-images. Other study also claimed [18] that an artificial neural network capable of supervised learning results in the creation of a surprisingly reliable predictor of steganographic content, even with relatively small amounts of embedded data. The interesting result is that clean color images can be reliably distinguished from steganographically

altered images based on texture alone, regardless of the embedding algorithm.

Another study [19] that utilized an artificial neural network as the classifier in a blind steganalysis system. They found that an artificial neural network performs better in steganalysis than Bayes classifier due to its powerful learning capability. Thus, IEEE Computer Society [20] has suggested artificial neural network technology system (ANNTS). This technology is designed to recognize the digital files containing messages hidden by scanning an image or other file. ANNTS can accurately identify steganographic images between 85% and 100% of the time.

c) Genetic Algorithm: Through a computational immune system (CIS) [21], a genetic algorithm approach has been used in blind steganography detection. They have developed a CIS classifiers, which evolved through a genetic algorithm (GA), that is able to distinguish between clean and stego images by using statistics gathered from a wavelet decomposition. A further study [22] has investigated an artificial immune system (AIS) approach to novel steganography detection for digital images. AIS typically mimic portions of the biological immune system (BIS) to provide a solution to a computational problem. Meanwhile, an application of genetic algorithm to optimal feature set selection in supervised learning using Support Vector Machine (SVM) for image steganalysis [23] has also presented. A genetic algorithm approach was used to optimize the feature set used by the classifier. Experimental results showed that the correct identification rates was as high as 98%, and as low as less than 2%.

d) Hybrid Method: There are two studies have been done on hybrid technique of image steganalysis [24, 25]. These studies have proven that the effectiveness of the AI hybrid in the dynamic environment is as good as Dynamic Evolving Neural Fuzzy Inference System (DENFIS) which was presented by [12].

3.2 Audio Steganalysis

Currently, interest in audio steganalysis is relatively low, despite obvious practical implications.

a) Bayesian: Echo coding is one of the most effective coding methods in terms of the signal-to-perceived noise ratio in audio steganography system. In Bayesian method, the process of distinguishing the audios with and without hidden data can be viewed as classification problem. Thus, a study [26] was carried out to detect hidden message by typical echo coding in audio steganalysis on statistical analysis of peak frequency with Bayes as a classifier. Experiments are conducted on a set of various types of audios and the correct rate of classification reaches to 80%. Compared with the method proposed by [27], this method is less time-consuming and gets high detecting accuracy for various embedding parameter combinations.

b) Neural Network: One of the audio steganalysis approach is using the principle of diminishing marginal distortions (DMD) [28]. This steganalysis technique is based on effect of repeated data embedding on the morphological structure of the audio signals. Thus, the principle of DMD is used to detect the presence of hidden messages in uncompressed audio files by using a single layer Feed Forward Neural Network (FFNN) for classification. Another study utilized a wavelet domain based on principal component analysis (PCA) [29] by using Radial Basis Function (RBF) network as a classifier. This scheme is used to detect the stego-audio signals embedded by wavelet domain LSB, Quantization Index Method (QIM) and Addition Method (AM). Simulation results show that the performances of the detection rates are all greater than 92%. This scheme does not only reduces the dimension of the feature vector effectively and simplifies the design of the classifier, but also keeps the detection performance high.

c) Genetic Algorithm: In audio steganalysis, GA is chosen because of its robustness to noise and no gradient information is required to find a global optimal. Spread Spectrum Watermarking (SSW) is one of the most interesting and powerful methods for embedding hidden information into audio signal. It is expected to have high degree of robustness, security and perceptual transparency. However, a study [10] has shown that the SSW approach has leak security for detecting exact location of watermark signal through an attack based on genetic algorithm. Besides that, the use of genetic algorithm [30] have explored to aid autonomous intelligent software agents capable of detecting any hidden information in audio files, automatically. This agent would create the Detection Agent (DA) in architecture comprising of several different agents that collaborate together to detect the hidden information. Another GA-based steganalysis approach called Stegobreaker [31] is proposed where the generated rules are used to classify audio documents in the real time environment. Experimental results showed that the Stegobreaker method worked effectively for the selected datasets and has the flexibility to be used to meet users' special requirements.

3.3 Video Steganalysis

Based on our survey currently, only one work on video steganalysis called Inter-frame Correlation Steganalysis [32]. This study proposed a blind steganalysis method to compress video stream by using a three layer Feed Forward Neural Network (FFNN) as the blind classifier. The features of the blind classifier are selected from the global DCT (discrete cosine transform) domain statistics in one single video scene on the collusion basis. Experimental results verify the availability of this scheme.

4 Conclusion

In this paper, we have addressed the implementation of computational intelligence in digital media. Three major methods of computational intelligence have been identified to be useful on steganalysis; they bayesian, neural network, and genetic algorithm. We have found that neural network is a popular choice for the image steganalysis while genetic algorithm is the first choice for audio steganalysis. In future work, we are considering the use of computational intelligence in natural language steganalysis environment.

References:

[1] R. Chandramouli, and S.K. Subbalakshmi, "Current Trends in Steganalysis: A Critical Survey," Control, Automation, Robotics and Vision Conference (ICARCV), vol. 2, pp 964–967, December 2004, ISBN: 0-7803-8653-1.

[2] S.L. Tanimoto, *The Elements of Artificial Intelligence : An Introduction Using LISP*, Computer Science Press Inc., 1803 Research Boulevard, Rockville, Maryland 20850, 1987, ISBN -88175-113-8.

[3] A.A. Hopgood, *Intelligent Systems for Engineers and Scientists, 2nd Edition*, CRC Press, 2001.

[4] S. Kumar, *Neural Networks - A Class Room Approach*, McGraw Hill, 2004.

[5] N.M. Martin, and L.C. Jain, *Introduction to Neural Network, Fuzzy systems, Genetic Algorithms, and their Fusion in Fusion of Neural Networks, Fuzzy Sets, and Genetic Algorithms : Industrial Applications*, International Series on Computational Intelligence, CRC Press, pp. 1–12, 1999.

[6] T. Fukuda, and K. Shimojima, "Hierarchical Intelligent Robotic System -Adaptation, Learning and Evolution," Proceeding of International Conference on Computational Intelligence and Multimedia Applications (ICCIMA'97), Gold Coast, Australia, pp.1-5, 1997.

[7] L.H. Tsoukalas, *Fuzzy and Neural Approaches in Engineering*, John Wiley and Sons Ltd, Canada, 1997.

[8] S. Goonatilake, and S. Khebbal, *Intelligent Hybrid Systems*, John Wiley & Sons Ltd, England, UK, 1995.

[9] R. Benton, and H. Chu, "LSB Embedding Steganalysis Using Neural Network, 3rd International Conference on Information Technology: Research and Education (ITRE 2005), Hsinchu, Taiwan, pp. 105-109, June 2005, ISBN: 0-7803-8933-6.

[10] S. Sedghi, H.R. Mashhadi, and M. Khademi, "Detecting Hidden Information from a Spread Spectrum Watermarked Signal by Genetic Algorithm," Congress on Evolutionary Computation (CEC '06), Vancouver, Canada, pp.173–178, July 2006, ISBN: 0-7803-9487-9.

[11] R. Ji, H. Yao, S. Liu, and L. Wang, "Genetic Algorithm Based Optimal Block Mapping Method for LSB Substitution," International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP '06), pp. 215-218, December 2006, ISBN: 0-7695-2745-0.

[12] Q. Liu, and A. H. Sung, "Feature Mining and Neuro-Fuzzy Inference System for Steganalysis of LSB Matching Steganography in Grayscale Images," Proceedings of the 20th International Joint Conference on Artificial Intelligence (IJCAI 2007), Hyderabad, India, pp. 2808-2813, January 2007.

[13] Q. Liu, and A. H. Sung, "Detect Information-Hiding Type and Length in Jpeg Images by Using Neuro-Fuzzy Inference Systems", Congress on Image and Signal Processing (CISP), Sanya, China, vol. 5, pp. 692-696, May 2008, ISBN: 987-0-7695-3119-9.

[14] A. Ambalavanan, and R. Chandramouli, "A Bayesian Image Steganalysis Approach to Estimate the Embedded Secret Message," International Multimedia Conference, Proceedings of the 7th Workshop on Multimedia and Security, ACM Press, New York, USA, pp. 33–38, 2005, ISBN: 1-59593-032-9.

[15] U.M. Sekarji, "Detection of Hidden Information in Images Using Neural Networks," SASTRA Tanjore, India, 2001, unpublished.

[16] S. Liu, H. Yao, and W. Gao, "Neural Network Based Steganalysis in Still Images,"

Proceedings of the 2003 International Conference on Multimedia and Expo (ICME 2003), vol.2, pp. II – 509–512, July 2003, ISBN: 0-7803-7965-9.

[17] S. Liu, H. Yao, and W. Gao, "Steganalysis Based on Wavelet Texture Analysis and Neural Network," *Fudan Journal (Natural Science)*, 43 vol. 5 (2004/10), pp. 910-913, 2004.

[18] P. Lafferty, and F. Ahmed, "Texture-based Steganalysis: Results for Color Images," Mathematics of Data/Image Coding, Compression, and Encryption VII, with Applications, Proceedings of the SPIE, vol. 5561, pp. 145-151, 2004.

[19] Y.Q. Shi, G. Xuan, D. Zou, J. Gao, C. Yang, Z. Zhang, P. Chai, W. Chen, and C. Chen, "Steganalysis Based on Moments of Characteristic Functions Using Wavelet Decomposition, Prediction-Error Image, and Neural Network," Conference on Multimedia and Expo (IEEE ICME 2005), Amsterdam, The Netherlands, July 2005.

[20] IEEE Computer Society, "New System Fights Steganography Purpose Artificial Neural Network Technology for Steganalysis (ANNTS)," August 2006. Available at http://www.computer.org/portal/cms_docs_computer/computer/homepage/0806/news_briefs.pdf

[21] J.T. Jackson, G.H. Gunsch, R.L. Claypoole, and G.B. Lamont, "Blind Steganography Detection Using a Computational Immune System: A Work In Progress," *International Journal of Digital Evidence*, issue 1, vol. 4, 2002.

[22] J.T. Jackson, G.H. Gunsch, R.L. Claypoole, and G.B. Lamont, "Novel Steganography Detection Using an Artificial Immune System Approach," Congress on Evolutionary Computation (CEC '03), vol. 1, pp. 139- 45, December 2003, ISBN: 0-7803-7804-0.

[23] T. Knapik, E. Lo , and J.A. Marsh, "Application of Genetic Algorithm to Steganalysis," Modeling and Simulation for Military Applications, Proceedings of the SPIE, vol. 6228, pp. 62280X, May 2006.

[24] T. Iba, and Y. Takefuji, "Adaptation of Neural Agent in Dynamic Environment: Hybrid System of Genetic Algorithm and Neural Network," Proceedings of the Second International Conference on Knowledge-Based Intelligent Electronic Systems (KES '98), Adelaide, SA, Australia, vol. 3, pp. 575-584, April 1998, ISBN: 0-7803-4316-6.

[25] I.S. Oh, J.S. Lee, and B.R. Moon, "Hybrid Genetic Algorithms for Feature Selection," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 26, issue 11, pp. 1424-1437, November 2004.

[26] W. Zeng, H. Ai, R. Hu, and S. Gao, "An Algorithm of Echo Steganalysis Based on Bayes Classifier," International Conference on Information and Automation (ICIA 2008), Changsha, China, pp. 1667-1670, June 2008, ISBN: 978-1-4244-2183-1.

[27] H. Ozer, I. Avcibas, B. Sankur, and N. Memon, "Steganalysis of Audio Based on Audio Quality Metrics," SPIE Electronic Imaging Conference on Security and Watermarking of Multimedia Contents, Santa Clara, vol. V, pp. 55–66, January 2003.

[28] O. Altun, G. Sharma, M. Celik, M. Sterling, E. Titlebaum, and M. Bocko, "Morphological Steganalysis of Audio Signals and the Principle of Diminishing Marginal Distortions," Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '05), Philadelphia, PA, USA, pp. 21-24, vol. 2, March 2005, ISBN: 0-7803-8874-7.

[29] J. Fu, Y. Qi, and J. Yuan, "Wavelet Domain Audio Steganalysis Based on Statistical Moments and PCA," Proceedings of the International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR '07), Beijing, China, vol. 4, pp. 1619-1623, November 2007, ISBN: 978-1-4244-1065-1.

[30] S.Geetha, S.S. Sivatha Sindhu, and A. Kannan, "An Active Rule Based Approach to Audio Steganalysis with a Genetic Algorithm," Proceedings of the IEEE 1st International Conference on Digital Information Management, Bangalore, India, pp. 131-136, December 2006, ISBN: 1-4244-0682-X.

[31] S. Geetha, S.S. Sivatha Sindhu, and A. Kannan, "StegoBreaker: Audio Steganalysis Using Ensemble Autonomous Multi-Agent and Genetic Algorithm," Annual India Conference, New Delhi, pp. 1-6, September 2006, ISBN: 1-4244-0369-3.

[32] B. Liu, F. Liu, and P. Wang, "Inter-Frame Correlation Based Compressed Video Steganalysis (2008)," Congress on Image and Signal Processing (CISP '08), Sanya, China, vol. 3, pp. 42-46, May 2008, ISBN: 978-0-7695-3119-9.