Proceeding of International Conference on Electrical Engineering, Computer Science and Informatics (EECSI 2015), Palembang, Indonesia, 19 -20 August 2015

Performance Analysis on Text Steganalysis Method Using A Computational Intelligence Approach

Roshidi Din,
Shafiz Affendi Mohd Yusof,
Angela Amphawan,
School of Computing
University Utara Malaysia, UUM
Sintok, Kedah, Malaysia
roshidi@uum.edu.my,
shafiz@uum.edu.my,
angela@uum.edu.my

Hanizan Shaker Hussain,
Hanafizah Yaacob,
Nazuha Jamaludin,
Department of Computer Science
Kolej Poly-Tech MARA, KPTM
Cheras, Kuala Lumpur, Malaysia
hanizan@gapps.kptm.edu.my,
hanafi@gapps.kptm.edu.my,
nazuha@gapps.kptm.edu.my

Azman Samsudin
School of Computer Sciences
University Sains Malaysia, USM
Gelugor, Pulau Pinang, Malaysia
azman@cs.usm.my

Abstract*— In this paper, a critical view of the utilization of computational intelligence approach from the text steganalysis perspective is presented. This paper proposes a formalization of genetic algorithm method in order to detect hidden message on an analyzed text. Five metric parameters such as running time, fitness value, average mean probability, variance probability, and standard deviation probability were used to measure the detection performance between statistical methods and genetic algorithm methods. Experiments conducted using both methods showed that genetic algorithm method performs much better than statistical method, especially in detecting short analyzed texts. Thus, the findings showed that the genetic algorithm method on analyzed stego text is very promising. For future work, several significant factors such as dataset environment, searching process and types of fitness values through other intelligent methods of computational intelligence should be investigated.

Keywords—genetic algorithm method; computational intelligence; steganography, text steganalysis; fitness function value; performance evaluation; statistical method

I. INTRODUCTION

The Information Hiding field have played a significant role in e-secret communication channel and e-business applications such as e-national security [1], e-military [2], multimedia property [3], and authentication application [4]. Most of the new attacks in information hiding called steganalysis are derived by analyzing hidden protocol techniques in order to detect and extract the hidden messages. Steganalysis is aimed at discovering the hidden message from useless covert messages on analyzed medium communication channels [5, 6]. Until recently, there are two types of methods in detecting the hidden message namely digital steganalysis and text steganalysis. Most of the digital steganalysis methods which are proposed by steganalyst can be divided into three major domains such as image steganalysis [7, 8, 9], audio steganalysis [10, 11], and video steganalysis [12, 13]. Besides that, text steganalysis method is used to discover the existence of hidden message on the features of characteristics, statistical probabilities or linguistic structures of natural language domain [14]. Currently, there are several detection methods in text steganalysis methods on natural language structure which is divided into six categories such as feature-based, statistical method, rhetorical, syntactical-based, lexical, and semantic-based [15, 16, 17, 18, 19, 20] as shown in Fig. 1.

From the theoretical point of view in text steganalysis [21], one of the challenges for steganalyst that need to be considered is to justify whether the analyzed text may or may not contain hidden messages that is embedded into them. Therefore, steganalyst does not know exactly that the analyzed text is a stego text. This means that the steganalyst cannot decide whether the analyzed text contains hidden message or not. This is because most of stego text "looks or feels" just like an innocent text even though it contains a hidden message. However, there are boundaries of solutions which text steganography method does not know how competent the steganalysis detectors are in measuring the steganography methods intelligently [21]. Thus, it seems like a hard challenge from steganalyst's point of view. It also raises an interesting question on deciding which intelligent method should be utilized in steganalytic system. As far as our knowledge is concerned, there has been little effort on the usage of text steganalytic system to utilize the computational intelligence method.

In the meantime, several studies have been applying intelligent methods such as genetic algorithm on digital steganalysis domain in order to find the hidden messages. Most of the results have proven that the utilization of genetic algorithm based system has performed exceptionally [22, 23].

Despite the different genetic algorithm methods on digital steganalysis domain that has been proposed, the potential of exploring the usage of genetic algorithm method in steganalysis for text domain is still under-utilized.

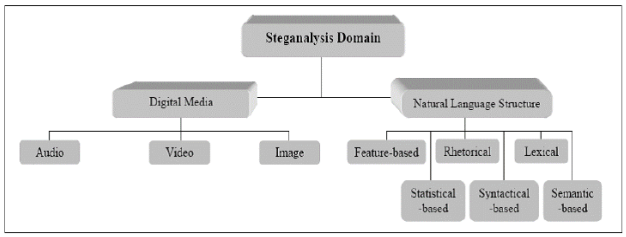

Fig. 1. A modern classification of steganalysis domain.

Hence, the motivation of this study is to utilize a genetic algorithm method in order to produce a good performance analysis on text steganalysis domain. Our primary goal is to analyze the performance between the genetic algorithm method and the statistical method in order to detect the hidden message on analyzed text. This paper is organized as follows. The next section deals with the discussion of intelligent methods of computational intelligence approach involved on text domain and digital steganalysis domain. This is then followed by the experimental design and the discussion of the results. Last, the concluding remarks will be given.

II. COMPUTATIONAL INTELLIGENCE ON TEXT STEGANALYSIS DOMAIN

Nowadays, there are four main intelligent methods of computational intelligence approach that have been applied in text processing domain. These are bayesian network, neural network, genetic algorithm, and fuzzy logic. All these methods are widely used in order to understand the human intelligence. Therefore, many steganalyst have applied computational intelligence approach on digital steganalysis domain. The discussion of these four intelligent methods on text and text steganalysis domain are summarized in TABLE I and TABLE II.

TABLE I. SUMMARY OF COMPUTATIONAL INTELLIGENCE METHODS ON TEXT DOMAIN.

Various Methods of Computational Intelligence Approaches		
Text Domain Types	**Researchers**	**Applied Domain**
Bayesian Network		**Document Classification**
	Kaza *et al*. [24] Hong-Bo *et al*. [25]	Pattern recognition. Stable classifier.
	Gama [26]; Shi *et al*. [27]	Classifier for document.
Neural Network		**Natural Language Processing**
	Roa & Nino [28]	Classify grammatical or ungrammatical of sentences.
	Ayan *et al*. [29] Schwenk & Gauvain [30]	Classifier with linguistic features. Large text corpora for language modelling.
Genetic Algorithm		**Natural Language Optimization**
	Dekkers [31]	Utilize a Optimality Theoretic Systems.
	Aycinena *et al*. [32]	Evolving natural language grammars.
	Wilson & Heywood [334]	Grammatical Components.
Fuzzy Logic		**Natural Language Representation**
	Haliday [34]	Context of metalanguage.
	Ralescu [35]	Fuzzy quantifiers on many occasions.
	Zadeh [36]	Terminal SET Data (TDS).
	Wang & Qiu [37]	Linguistic description by virtue of propositions.
	Barone & Dewan [38]	Fuzzy grammatics with theory of language .
	Barro *et al*. [39]	Fuzzy quantifiers in the language of daily life.
	Zadeh [40]	Computing with words through Generalized Constraint Language.

In TABLE I and TABLE II, computational intelligence methods on text domain and the usage of computational intelligence methods in digital steganalysis are summarized. It has been identified that genetic algorithm and fuzzy logic are the most capable method to apply on natural language environment. However, genetic algorithm is a bestfit computational intelligence method in producing a systematic rule for feature selection of solution and very powerful for optimization in text domain. In addition, it has been identified as well to pass the detection of current steganalytic systems on digital domain and also worked effectively on audio steganalysis and image steganalysis. Thus, this study believes that the genetic algorithm method can be applied intelligently and will perform well on text steganalysis domain.

TABLE II. SUMMARY OF COMPUTATIONAL INTELLIGENCE METHODS ON DIGITAL STEGANALYSIS DOMAIN.

Digital Steganalysis Methods			
Domain Types	**Image**	**Video**	**Audio**
Bayesian Network	Bayesian Framework [41]		Statistical Moments of Peak Frequency [42]
Neural Network	Characteristic Functions [43]		Principle of Diminishing Marginal Distortions [44]
	Combination of Triple Features [45]	Inter-frame Correlation [46]	
Genetic Algorithm	Computational Immune System [47]		
	Genetic Algorithm Based Methodology [48]		Classification Rules Quality [49]
Hybrid	Dynamic Evolving Neural Fuzzy Inference System - DENFIS [50]		
	JPEG Steganalysis through Neuro-Fuzzy Inference System [51]		

III. EXPERIMENTAL DESIGN

There are four stages involved in the experimental design such as the preprocessing of dataset used, text genome initialization, genetic algorithm detection engine and performance evaluation. The experimental design of this study is illustrated in Fig. 2.

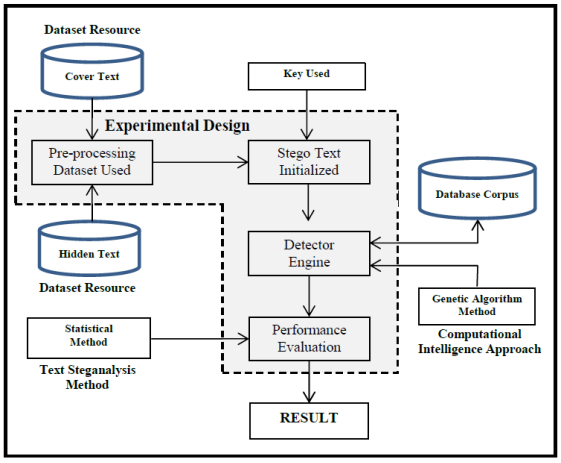

Fig. 2. An experimental design for text steganalysis domain.

The first stage can be assumed as a setting up step which is to justify the collection of datasets used in this study. It utilizes

a hidden dataset of analyzed text [52] containing 10 lines with 893 bytes. It also uses a cover text from an established database known as Reuters News 21578. Besides, a detection process uses an established Oxford dictionary as a database corpus in order to verify the words or sentences on analyzed text. Actually, the system does not know what words or sentences included in each line of the sentences of an analyzed text before the detection process is done. Once the system receives an analyzed text, it will pass on an analyzed text during detecting process.

Then, second stage is an initialization of stego text. The role of this stage is to initialize the genes features of text genome. It is based on the rules features of the cover text Tc, hidden text Tm and the stego key used, Kn. In this process, each of the hidden text, Tm is embedded into cover text Tc using stego key used Kn which is known as embedding process. The purpose of this stage is to produce a stego text in order to be used as analyzed text Tn with the fitness function values fn. This information can be used as an input to detection process which utilizes a genetic algorithm method.

Next, the third stage consists of genetic algorithm detector. A development system of genetic algorithm detector uses JAVA Genetic Algorithm Programming (JGAP) language with interface under NetBeans IDE 6.9.1 environment. In this stage, the patterns and the behaviours of the analyzed text Tn are studied as much as it could due to understanding the analyzed text Tn itself through a database corpus using genetic algorithm detector. The searching process will end whenever genetic algorithm detector gets optimum estimated values namely cost function values of analyzed text Tn.

As a final stage, performance evaluation is to measure the score values of several parameters between genetic algorithm method and statistical method. Finally, the results of these parameters will be discussed.

IV. RESULT AND DISCUSSION

The purpose of this section is to analyze the results of the performance of statistical method versus genetic algorithm method during the extraction of a hidden message from a cover text. There are five metric parameters used in this experiment such as running time, best fitness value, mean distributions, variance distributions and standard deviation distributions. These metric parameters were investigated on 100 cover texts files of dataset. The score values of these five metric parameters are shown from Fig. 3 until Fig. 7.

A. Running Time

Based on Fig. 3, the results showed that the running time for both methods fluctuates between 3 and close to 60 seconds. However, the running time of statistical method is almost higher than the running time of genetic algorithm method. It may be influenced by the searching process of the corpus used in good environmental datasets. Only several texts of the genetic algorithm method had sudden spikes which were at the running time of texts 60, 98, and 99. Thus, it is found that the running time performance of genetic algorithm method is more stable than the statistical method for good environmental datasets.

B. Fitness Values

The results showed that the best fitness performance for both methods fluctuates nearly between 14 and 40 of cost value which is plotted in Fig. 4. The range of the best fitness performance using statistical method is between 18 and 40 of cost value whereas the range of best fitness performance using genetic algorithm method is between 14 and 28 of cost value. Therefore, it is found that the best fitness performance for genetic algorithm method is better than the statistical method for the good dataset environment.

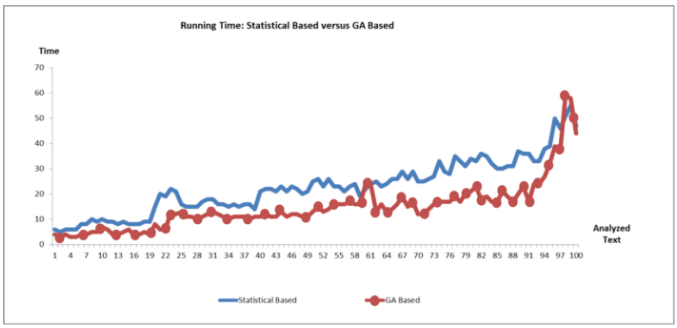

Fig. 3. A performance of running time for statistical based versus GA based.

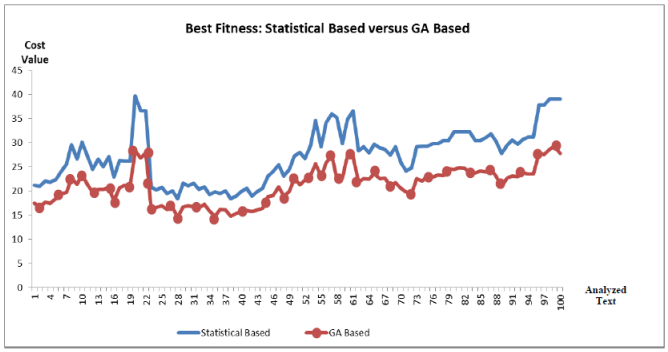

Fig. 4. A performance of best fitness for statistical based versus GA based.

C. Probability of Mean

The results showed that the mean probability of statistical based method sustainably fluctuates from close to 0.65 to 0.9 which is demonstrated in Fig. 5. However, the mean probability of genetic algorithm method remains constant closely at 1. Therefore, the mean probability of statistical method is lower than the mean probability of genetic algorithm method. The results of mean distribution measurements for statistical method and genetic algorithm method showed that the mean distribution for genetic algorithm method has a smaller range and is more accurate compared to the statistical method for good dataset environment.

D. Probability of Variance

Based on Fig. 6, the results showed that the variance probability of statistical method fluctuates from close to 0.01 to 0.023. However, the variance probability of genetic algorithm method remains unchanged closely to 0. Therefore, the

variance probability of statistical method is higher than the variance probability of genetic algorithm method. The results of variance distribution measurement for statistical method and genetic algorithm method show that the variance distribution for genetic algorithm method has a smaller range and accurate than the statistical method for good dataset environment.

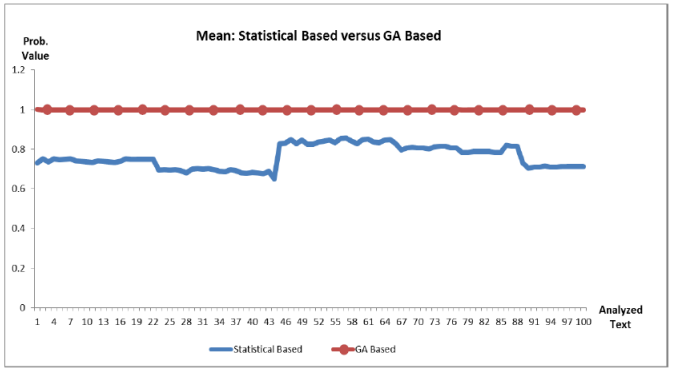

Fig. 5. A mean probability of statistical based versus GA based.

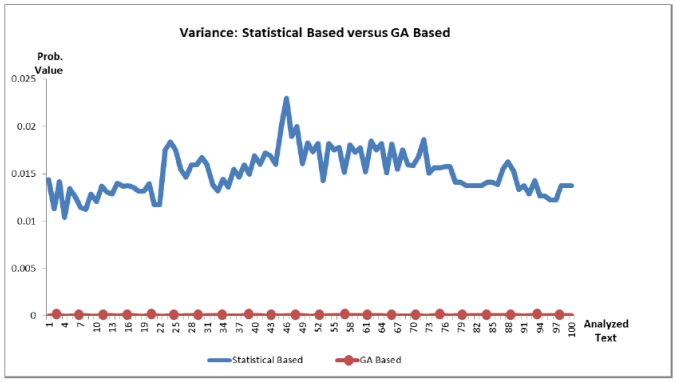

Fig. 6. A probability of variance for statistical based versus GA based.

E. Probability of Standard Deviation

The results showed that the standard deviation probability of statistical based method fluctuates from close to 0.01 to 0.015 which is presented in Fig. 7. However, the standard deviation probability of genetic algorithm method remains unchanged at 0. Therefore, the standard deviation probability of statistical based method is higher than the standard deviation probability of genetic algorithm method. The results of standard deviation distribution measurement for statistical method and genetic algorithm method showed that the standard deviation distribution for genetic algorithm method has a smaller range and is more accurate compared to the statistical method for good dataset environment.

V. CONCLUSION

The primary contribution of this paper is to present the usage of computational intelligence approach works which in return would contribute to text steganalysis domain. The work presented here is among the earliest effort on text steganalysis domain using computational intelligence approach. It justifies that the genetic algorithm method perform better compared to statistical method based on used parameter metrics in order to identify hidden message on an analyzed text. For future work, it is suggested the several factors such as dataset environment, searching process, and types of fitness values should be considered in order to increase the strength of steganalysis method on text domain. Besides, the use of other computational intelligence method such as neural network, fuzzy evaluation, swarm optimization, and ant colony optimization should be explored and investigated.

ACKNOWLEDGMENT

We would like thank to Assoc. Prof. Dr. Huda Ibrahim, Dean of School of Computing, Universiti Utara Malaysia (SoC CAS UUM) and Director of Research and Innovation Management Centre (RIMC) for their moral support for the realization of this work. This research was financially supported by the High Performance Individual Research Grant National (Grant NO. 37011) under RIMC Grant, Universiti Utara Malaysia (UUM).

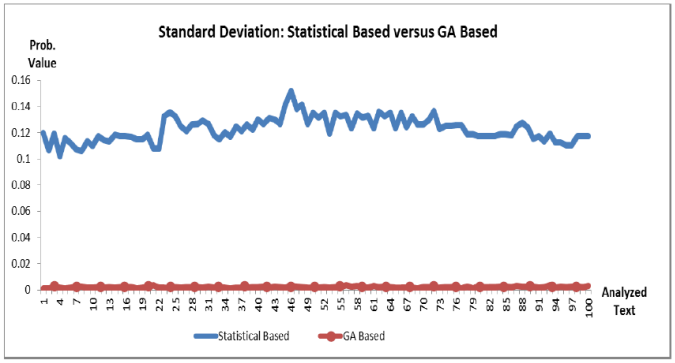

Fig. 7. A probability of standard deviation for statistical based versus GA based.

REFERENCES

[1] H. Si and C.T. Li, Maintaining information security in e-government through steganology, Department of Computer Science, University of Warwick, UK, 2008.

[2] R. Din and A. Samsudin, "Digital steganalysis: computational intelligence approach," International Journal of Computers, vol. 3, no. 1, pp. 161-170, 2009.

[3] Y. Perwej, P. Firoj and A. Perwej, "An adaptive watermarking technique for the copyright of digital images and dgital image protection," The International Journal of Multimedia & Its Applications (IJMA), vol. 4(2), pp. 21-38, 2012.

[4] S. Gunawardena, D. Kulkarni and B. Gnanasekaraiyer, "A steganography-based framework to prevent active attacks during user authentication," IEEE 8th International Conference on Computer Science & Education (ICCSE), 2013, pp. 383-388.

[5] L. He, X. Gui, R. Wu, B. Xie and C. Hu, "A hybrid natural language information hiding system," Electronics and Electrical Engineering, vol. 18, no. 9, pp. 95-100, 2012.

[6] K. Bryan, "Video steganalysis for digital forensics investigation," Open Access Dissertations, Paper 48, 2013. http://digitalcommons.uri.edu/oa_diss/48

[7] N. Hamid, A. Yahya, R. B. Ahmad and O.M. Al-Qershi, "Image steganography techniques: an overview," International Journal of Computer Science and Security (IJCSS), vol. 6, no. 3, pp. 168-187, 2012.

[8] C. Wang and J. Ni, "An efficient JPEG steganographic scheme based on the block entropy of DCT coefficients," IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2012, pp. 1785-1788.

[9] K. Choudhary, "Image steganography and global terrorism," International Journal of Scientific & Engineering Research, vol. 3(7), pp. 1-12, 2012.

[10] . Zamani, , A. A. Manaf and S. M. Abdullah, "Efficient embedding for audio steganography," 2nd International Conference on Environment, Economics, Energy, Devices, Systems, Communications, Computers, Mathematics (EDSCM'13), 2012, pp. 195-199.

[11] K. P. Adhiyaand and S. A. Patil, "Hiding text in audio using LSB based steganography, " Information and Knowledge Management, vol. 2, no. 3, pp. 8-14, 2012.

[12] P. V. Bodhak and B. L. Gunjal, "Improved protection in video steganography using DCT & LSB," International Journal of Engineering and Innovative Technology, vol. 1, no. 4 pp. 31-37, 2012.

[13] K. Dasgupta, J. K. Mandal and P. Dutta, "Hash based least significant bit technique for video steganography (HLSB), " International Journal of Security, Privacy and Trust Management (IJSPTM), vol. 1, no. 2, pp. 1-10, 2012.

[14] R. Chandramouli and N. D. Memon, "Steganography capacity: a steganalysis perspective," Proc. SPIE Security and Watermarking of Multimedia Contents, 2003.

[15] X. Lingyun, S. Xingming, L. Gang and G. Can, "Research on steganalysis for text steganography based on font format," 3rd International Symposium on Information Assurance and Security, 2007, pp. 490 - 495.

[16] I. Nechta and A. Fionov, "Applying statistical methods to text steganography," CoRR, October, 2011.

[17] F. Fukumoto and Y. Suzuki, "Extracting key paragraph based on topic and event detection - towards multi-document summarization," ANLP/NAACL Workshops, NAACL-ANLP 2000 Workshop on Automatic Summarization, Seattle, Washington, vol. 4, pp. 31 – 39, 2000.

[18] H. Yang and X. Cao, "Linguistic steganalysis based on meta features and immune mechanism," Chinese Journal of Electronics, vol. 19(4), pp. 661 - 666, 2010.

[19] C. M. Taskiran, U. Topkara, M. Topkara, and E. J. Delp, "Attacks on lexical natural language steganography systems," Proceeding of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents, San Jose, 2006, pp. 15 – 19.

[20] M. Alfonso, C. Justo and A. A. Irina, "Measuring the security of linguistic steganography in spanish based on synonymous paraphrasing with WSD," 10th IEEE International Conference on Computer and Information Technology (CIT 2010), 2010, pp. 965 - 970.

[21] R. Din, Z. Che Ani and A. Samsudin, "A formulation of conditional states on steganalysis approach," WSEAS Transactions on Mathematics, vol. 11, no. 3, pp. 173-182, 2012.

[22] S. Geetha, S.S. A. S. Sindhu and Kannan, "StegoBreaker: audio steganalysis using ensemble autonomous multi-aAgent and genetic algorithm," Annual IEEE India Conference, 2006, pp. 1 – 6.

[23] A. M. Fard, M. R. Akbarzadeh-T and F. Varasteh-A, "A new genetic algorithm approach for secure JPEG steganography," IEEE International Conference on Engineering of Intelligent Systems, 2006, pp. 1 – 6.

[24] S. Kaza, S. N. J. Murthy and G. Hu, "Identification of deliberately doctored text documents using frequent keyword chain (FKC) model," Proceeding of IRI, vol. 3, pp. 98 – 405, 2003.

[25] S. Hong-Bo, W. Zhi-Hai and H. Hou-Kuan and L.P. Jing, "Text classification based on the TAN model," Proceeding of IEEE TENCON'02, vol. 1, pp. 43-46, 2002.

[26] J. Gama, "A linear-bayes classifier, " Advances in Artificial Intelligence, Springer Berlin Heidelberg, 2000, pp. 269-279.

[27] H. F. Shi, T. G. Fanand and G. L. Zhang, "Documents categorization based on bayesian spanning tree," Proceedings of The Fifth International Conference On Machine Learning And Cybernetics, Dalian, China, 2006, pp. 1072 – 1075.

[28] S. Roa and F. Niño, "Classification of natural language sentences using neural networks," Proceedings of the Sixteenth International Florida Artificial Intelligence Research Society (FLAIRS) Conference, 2003, pp. 444-449.

[29] N. F. Ayan, B. J. Dorr and C. Monz, "Neuralign: combining word alignments using neural networks," Proceedings of the conference on Human Language Technology and Empirical Methods in Natural Language Processing Association for Computational Linguistics, 2005, pp. 65-72.

[30] H. Schwenk and J. L. Gauvain, "Training neural network language models on very large corpora," Proceedings of the conference on Human Language Technology and Empirical Methods in Natural Language Processing, Association for Computational Linguistics, 2005, pp. 201-208.

[31] J. Dekkers, F. R. H. van der Leeuw and J. M. van de Weijer, Optimality theory: phonology, syntax, and acquisition, Oxford University Press. (Eds.), 2000.

[32] M. Aycinena, M. Aycinena and D. Mulford, An evolutionary approach to natural language grammar induction, Stanford CS 224N Natural Language Processing, 2003.

[33] G. Wilson and M. Heywood, "Use of a genetic algorithm in brill's transformation-based part-of-speech tagger," Proceedings of the Conference on Genetic and Evolutionary Computation, ACM, 2005, pp. 2067-2073.

[34] M. A. K. Halliday, "Fuzzy grammatics: a systemic functional approach to fuzziness in natural language," Proceedings of IEEE International Joint Conference of the 4th IEEE International Conference on Fuzzy Systems and The 2nd International Fuzzy Engineering Symposium, vol. 1, pp. 9-26, 1995.

[35] A. L. Ralescu, "Cardinality, quantifiers, and the aggregation of fuzzy criteria," Fuzzy Sets System, vol. 69, pp. 355–365, 1995.

[36] L. A. Zadeh, "Fuzzy logic - computing with words," IEEE Transactions on Fuzzy Systems, vol. 4(2), pp. 103-111, 1996.

[37] H. Wang and D. Qiu, "Computing with words via turing machines: a formal approach," IEEE Transactions on Fuzzy Systems, vol. 11(6), 2003, pp. 742-753.

[38] J. M. Barone and P. Dewan, "Looking for fuzziness in natural language," Fuzzy Information Processing Society, 22nd International Conference of the North American, 2003, pp. 26-31.

[39] S. Barro, A. J. Bugarin, P. Cariñena and F. Díaz-Hermida, "A framework for fuzzy quantification models analysis," IEEE Transactions on Fuzzy Systems, vol. 11(1), 2003, pp. 89-99.

[40] L. A. Zadeh, "The concept of a generalized constraint-a bridge from natural languages to mathematics," Fuzzy Information Processing Society, Annual Meeting of the North American, 2005, pp. 1-6.

[41] 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, 2005, pp. 33 –38.

[42] 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, June 2008, pp. 1667-1670.

[43] 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.

[44] 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, vol. 2, pp. 21 – 24, March 2005.

[45] 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.

[46] B. Liu, F. Liu and P. Wang, "Inter-frame correlation based compressed video steganalysis," Congress on Image and Signal Processing (CISP '08), Sanya, China, vol. 3, pp. 42 – 46, May 2008.

[47] 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, vol. 4(1), 2002.

[48] Y. Wu and F.Y. Shih, "Genetic algorithm based methodology for breaking the steganalytic systems," IEEE Transactions on Systems, Man and Cybernetics, Computer Vision Lab., New Jersey Institute of Technol., Newark, NJ, USA, vol. 36(1), pp. 24 – 31, February 2006.

[49] 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, December 2006, pp. 131 - 136.

[50] 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, January 2007, pp. 2808 - 2813.

[51] 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.

[52] C. Lyon, The representation of natural language to enable neural networks to detect syntactic structures, PhD Thesis, University of Hertfordshire, 1994.