I. J. Computer Network and Information Security, 2013, 12, 45-52
Published Online October 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.12.06

Study and Analysis of Text Steganography Tools

Indradip Banerjee
Department of Computer Science & Engineering, National Institute of Technology,
Durgapur, West Bengal, India.
ibanerjee2001@yahoo.com

Souvik Bhattacharyya
Department Computer Science & Engineering,University Institute of Technology,
Burdwan University, Burdwan, India
souvikbha@gmail.com

Gautam Sanyal
Department of Computer Science & Engineering, National Institute of Technology,
Durgapur, West Bengal, India.
nitgsanyal@gmail.com

Abstract — "Maintain the security of the secret information", this words has been a great challenge in our day to day life. Sender can send messages regularly through a communication channel like Internet, draws the attention of third parties, hackers and crackers, perhaps causing attempts to break and expose the unusual messages. Steganography is a gifted region which is used for secured data transmission over any public media. Wide quantity of research work has been established by different researchers on steganography. Steganalysis is an art and science of detecting messages hidden using steganography. Some research work has also been remarked in the field of Steganalysis also. In this contribution, we have gone through steganalysis attack of some established text steganography tools.

Index Term — Text Steganography, Text Steganalysis, Security, Cover Text, Stego Text

I. INTRODUCTION

Information hiding is the ability to prevent or hidden certain aspects from being accessible to others excluding authentic user. It has many sub disciplines. One of the most important sub disciplines is steganography [1] which is derived from a work by Johannes Trithemus (1462-1516) entitled "Steganographia" and comes from the Greek language defined as "covered writing" [2]. It is an ancient art of hiding information in ways a message is hidden in an innocent-looking cover media so that will not arouse an eavesdropper's suspicion. Steganography diverges from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret by encryption technique, steganography focuses on keeping the presence of a message secret [3], [4].

Another form of information hiding is digital watermarking, which is the process that embeds data called a watermark, tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image, audio, video or text only [5], [6]. A hidden channel could be defined as a communications channel that transfers some kind of information using a method originally not intended to transfer this kind of information. Observers are unaware that a covert message is being communicated. Only the sender and recipient of the message notice it. Steganography works have been carried out on different media like images, video clips, text, music and sound [7], [4].

In Image Steganography method the secret message is embedded into an image as noise to it, which is nearly impossible to differentiate by human eyes [8], [9], [10]. In video steganography, same method may be used to embed a message [11], [12]. Audio steganography embeds the message into a cover audio file as noise at a frequency out of human hearing range [10]. One major category, perhaps the most difficult kind of steganography is text teganography or linguistic steganography because due to the lack of redundant information in a text compared to an image or audio. The text steganography is a method of using written natural language to conceal a secret message as defined by Chapman et al. [13].

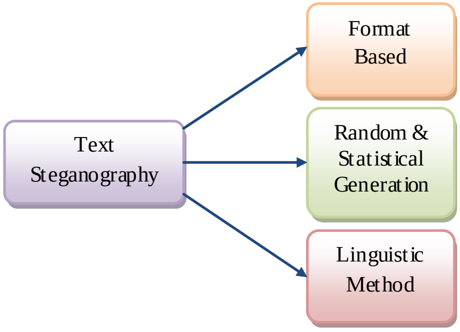


Figure 1: Types of Steganography

TEXT STEGANOGRAPHY

The affluence of electronic documented information available in the world as well as the exertion of serious linguistic analysis makes this an interesting medium for steganographic information hiding. Moreover the Text is one of the ancient media used in steganography. Letters, books and telegrams hide secret messages within their texts in earlier time i.e. before the electronic age comes. Text steganography refers to the hiding of information within text i.e. character-based messages. There are three basic categories of text steganography (Fig. 1) maintained here: format-based methods, random and statistical generation and linguistic methods.[14]

i. Format-based methods [14]: This methods use the physical formatting of text as a space in which to hide information. Format-based methods usually modify existing text for hiding the steganographic text. Insertion of spaces or non-displayed characters, careful errors tinny throughout the text and resizing of fonts are some of the many format-based methods used in text steganography.

ii. Random and statistical generation method [14]: This avoid comparison with a known plaintext, steganographers often resort to generating their own cover texts. Character sequences method hide the information within character sequences.

iii. Linguistic methods [14]: The affluence of electronic documented information available in the world as well as the exertion of serious linguistic analysis makes this an interesting medium for steganographic information hiding.

In case of text steganography, firstly, a secret message will be covered up in a cover-text by applying an embedding algorithm to produce a stego-text. The stego-text will then be transmitted by a communication channel to a receiver.

TEXT STEGANALYSIS

The usage of text media, as a cover channel for secret communication, has drawn more attention [15]. This attention in turn creates increasing concerns on text steganalysis. At present, it is harder to find secret messages in texts compared with other types of multimedia files, such as image, video and audio [16-21]. In general, text steganalysis exploits the fact that embedding information usually changes some statistical properties of stego texts; therefore it is vital to perceive the modifications of stego texts. Previous work on text steganalysis could be roughly classified into three categories: format- based [22, 23], invisible character-based [24-26] and linguistics, respectively. Different from the former two categories, linguistic steganalysis attempts to detect covert messages in natural language texts. In the case of linguistic steganography, lexical, syntactic, or semantic properties of texts are manipulated to conceal information while their meanings are preserved as much as possible[27].Due to the diversity of syntax and the polysemia of semantics in natural language, it is difficult to observe the alterations in stego texts. So far, many linguistic steganalysis methods have been proposed. In these methods, special features are designed to extend semantic or syntactical changes of stego texts. For example, Z.L. Chen [28] et al. designed the N-window mutual information matrix as the detection feature to detect semantic steganagraphy algorithms. Furthermore, they used the word entropy and the change of the word location as the semantic features [29, 30], which improved the detection rates of their methods. Similarly, C.M. Taskiran et al [31] used the probabilistic context-free grammar to design the special features in order to attack on syntax steganography algorithms. In the work mentioned above, designed features strongly affect the final performances and they can merely reveal local properties of texts. Consequently, when the size of a text is large enough, differences between Natural texts (NTs) and Stego texts (STs) are evident, thus the detection performances of the mentioned methods are acceptable. Whereas, when the sizes of texts become small, the detection rates decrease dramatically and cannot be satisfied for applications. In addition, some steganographic tools have been improved in the aspects of semantic and syntax for better camouflage [32]. Therefore, linguistic steganalysis still needs further research to resolve these problems. Some more work on Text Steganalysis has been discussed below.

A. Linguistic Steganalysis Based on Meta Features and Immune Mechanism [33]: Linguistic steganalysis depends on efficient detection features due to the diversity of syntax and the polysemia of semantics in natural language processing. This paper presents a novel linguistics steganalysis approach based on Meta features and immune clone mechanism. Firstly, Meta features are used to represent texts. Then immune clone mechanism is exploited to select appropriate features so as to constitute effective detectors. Our approach employed Meta features as detection features, which is an opposite view from the previous literatures. Moreover, the immune training process consists of two phases which can identify respectively two kinds of stego texts. The constituted detectors have the capable of blind steganalysis to a certain extent. Experiments show that the proposed approach gets better performance than typical existing methods, especially in detecting short texts. When sizes of texts are confined to 3kB, detection accuracies have exceeded 95.

B. Research on Steganalysis for Text Steganography Based on Font Format [34]: In the research area of text steganography, algorithms based on font format have advantages of great capacity, good imperceptibility and wide application range. However, little work on steganalysis for such algorithms has been reported in the literature. Based on the fact that the statistic features of font format will be changed after using font-format-based steganographic algorithms, we present a novel Support Vector Machine-based steganalysis algorithm to detect whether hidden information exists or not. This algorithm can not only effectively detect the existence of hidden information, but also estimate the hidden information length according to variations of font attribute value. As shown by experimental results, the detection accuracy of our algorithm reaches as high as 99.3 percent when the hidden information length is at least 16 bits.

The dimensionality of data from text file is normally huge; it is unrealistic to use the data directly for steganalysis. A feasible approach is to extract certain amount of data from the text and use them to represent the text itself for steganalysis. The features for steganalysis should reflect minor distortions associated with data hiding.

Moments based Feature

To construct the features of both cover and stego or suspicious text several moments of the series has been computed. In mathematics, a moment is, loosely speaking, a quantitative measure of the shape of a set of points. The "second moment", for example, is widely used and measures the "width" of a set of points in one dimension or in higher dimensions measures the shape of a cloud of points as it could be fit by an ellipsoid. Other moments describe other aspects of a distribution such as how the distribution is skewed from its mean, or peaked. There are two ways of viewing moments [35], one based on statistics and one based on arbitrary functions such as $f(x)$ or $f(x, y)$.

Statistical view: Moments are the statistical expectation of certain power functions of a random variable. The most common moment is the mean which is just the expected value of a random variable as given in 1.

$$\mu = E[X] = \int_{-\infty}^{\infty} xf(x)dx \qquad (1)$$

where $f(x)$ is the probability density function of continuous random variable X. More generally, moments of order p = 0, 1, 2, … can be calculated as $m_p = E[X^p]$.These are sometimes referred to as the raw moments. There are other kinds of moments that are often useful. One of these is the central moments $\mu_p = E[(X-\mu)^p]$. The best known central moment is the second, which is known as the variance, given in 2.

$$\sigma^2 = \int (x-\mu)^2 f(x)dx = m_2 - \mu_1^2 \qquad (2)$$

Two less common statistical measures, skewness and kurtosis, are based on the third and fourth central moments. Moments are easily extended to two or more dimensions as shown in 3.

$$m_{pq} = E[X^pY^q] = \iint x^p y^q f(x,y)dxdy \quad \ldots(3)$$

Here $f(x, y)$ is the joint pdf.

Estimation: However, moments are easy to estimate from a set of measurements, x_i. The p-th moment is estimated as given in 4 and 5.

$$m_p = \frac{1}{N}\sum_{i-1}^{N} x_i^p \qquad (4)$$

(Often $1/N$ is left out of the definition) and the p-th central moment is estimated as

$$\mu_p = \frac{1}{N}\sum_i (x_i - \bar{x})^p \qquad (5)$$

$\bar{x}$ is the average of the measurements, which is the usual estimate of the mean. The second central moment gives the variance of a set of data $s^2 = \mu_2$. For multidimensional distributions, the first and second order moments give estimates of the mean vector and covariance matrix. The order of moments in two dimensions is given by $p+q$, so for moments above 0, there is more than one of a given order. For example, m_{20}, m_{11}, and m_{02} are the three moments of order 2.

Non-statistical view: This view is not based on probability and expected values, but most of the same ideas still hold. For any arbitrary function $f(x)$, one may compute moments using the equation 6 or for a 2-D function using 7.

$$m_p = \int_{-\infty}^{\infty} x^p f(x)dx \qquad (6)$$

$$m_{pq} = \iint x^p y^q f(x,y)dxdy \qquad (7)$$

Notice now that to find the mean value of $f(x)$, one must use m_1/m_0, since $f(x)$ is not normalized to area 1 like the pdf. Likewise, for higher order moments it is common to normalize these moments by dividing by m_0 (or m_{00}). This allows one to compute moments which depend only on the shape and not the magnitude of $f(x)$. The result of normalizing moments gives measures which contain information about the shape or distribution (not probability dist.) of $f(x)$.

Digital approximation: For digitized data, we must replace the integral with a summation over the domain covered by the data. The 2-D approximation is written in 8.

$$m_{pq} = \sum_{i-1}^{M}\sum_{j-1}^{N} f(x_i, y_j)x_i^p y_j^q = \sum_{i-1}^{M}\sum_{j-1}^{N} f(i,j)i^p j^q \qquad (8)$$

If $f(x, y)$ is a binary matrix function of an object, the area is m_{00}, the x and y centroids are 9 and 10.

$$\bar{x} = m_{10} / m_{00} \qquad (9)$$

$$\bar{y} = m_{01} / m_{00} \quad \dots \quad (10)$$

To implement the attack of text Steganography we use some stego text from some available steganography tools which are discussed below.

SNOW DOS 32 [37]: The encoding system used by **snow** depend on the fact that spaces and tabs (known as *whitespace*), when appearing at the end of lines, are invisible when presented in pretty well all text viewing programs. This allows messages to be hidden in ASCII text without affecting the text's visual representation. And since trailing spaces and tabs occasionally occur naturally, their existence should not be sufficient to immediately alert an observer who stumbles across them.

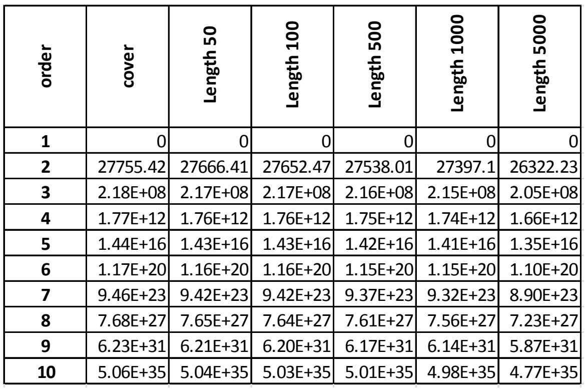
wbStego4.3open [36]: This module of steganography has been published under the GNU General Public License (GPL). wbStego uses a custom mechanism for localization. All information is stored in the data file, which consists of a number of blocks, all introduced by a 3 byte header specifying the size of the block. The file is a terminated by 3 bytes set to 0, i.e. a block header without data block.

In this paper, we have analyzed the text steganalysis by the help of statistical moment's technique using two of steganography tools. After wide research on steganography by author's previous work [11], [12], [13], [14], [15], [16], [17], [18], [33], [34], author is going to start work on the analysis part of text steganography.

This paper is organized into the following sections. Section II describes the proposed model. Analyses of the results are in section III. The last section descries the concluded part of the work.

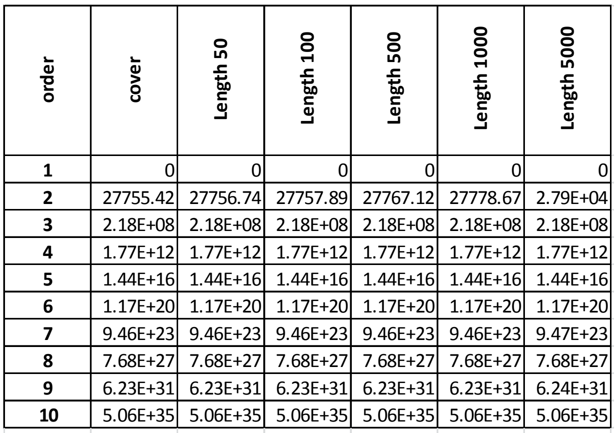
II. Proposed Model

Text steganalysis, at all this paper exactly deals with, uses two steganography tools (SNOW DOS 32 and wbStego4.3open). We have selected a cover and then create stego text by inserting various length of secret message. After that find out the moments up to 10 orders and observed that wbStego4.3open is better than SNOW DOS 32 at the side of embedding capacity.



order	cover	Length 50	Length 100	Length 500	Length 1000	Length 5000
1	0	0	0	0	0	0
2	27755.42	27666.41	27652.47	27538.01	27397.1	26322.23
3	2.18E+08	2.17E+08	2.17E+08	2.16E+08	2.15E+08	2.05E+08
4	1.77E+12	1.76E+12	1.76E+12	1.75E+12	1.74E+12	1.66E+12
5	1.44E+16	1.43E+16	1.43E+16	1.42E+16	1.41E+16	1.35E+16
6	1.17E+20	1.16E+20	1.16E+20	1.15E+20	1.15E+20	1.10E+20
7	9.46E+23	9.42E+23	9.42E+23	9.37E+23	9.32E+23	8.90E+23
8	7.68E+27	7.65E+27	7.64E+27	7.61E+27	7.56E+27	7.23E+27
9	6.23E+31	6.21E+31	6.20E+31	6.17E+31	6.14E+31	5.87E+31
10	5.06E+35	5.04E+35	5.03E+35	5.01E+35	4.98E+35	4.77E+35

Figure 2: Moment values of SNOW DOS 32 up to 10th order.



order	cover	Length 50	Length 100	Length 500	Length 1000	Length 5000
1	0	0	0	0	0	0
2	27755.42	27756.74	27757.89	27767.12	27778.67	2.79E+04
3	2.18E+08	2.18E+08	2.18E+08	2.18E+08	2.18E+08	2.18E+08
4	1.77E+12	1.77E+12	1.77E+12	1.77E+12	1.77E+12	1.77E+12
5	1.44E+16	1.44E+16	1.44E+16	1.44E+16	1.44E+16	1.44E+16
6	1.17E+20	1.17E+20	1.17E+20	1.17E+20	1.17E+20	1.17E+20
7	9.46E+23	9.46E+23	9.46E+23	9.46E+23	9.46E+23	9.47E+23
8	7.68E+27	7.68E+27	7.68E+27	7.68E+27	7.68E+27	7.68E+27
9	6.23E+31	6.23E+31	6.23E+31	6.23E+31	6.23E+31	6.24E+31
10	5.06E+35	5.06E+35	5.06E+35	5.06E+35	5.06E+35	5.06E+35

Figure 3: Moment values of wbStego4.3open up to 10th order.

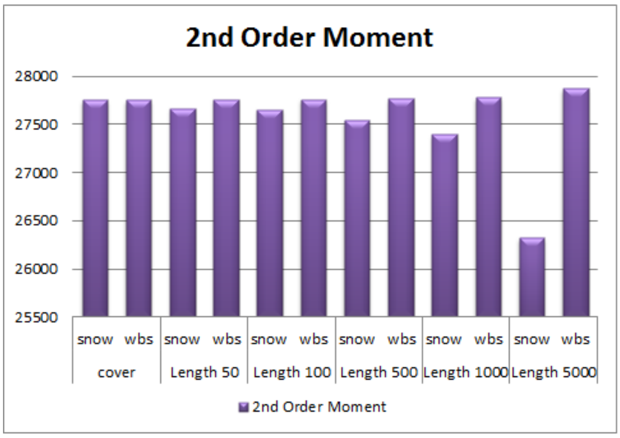


Figure 4: 2nd Order Moment values of SNOW & wbStego4.3open.

Here we have observed that the value of moment in various length has changes. Simultaniously it also occurs in between 2nd order moment to 10th order moment which is furnished in Figure 2 and Figure 3 of SNOW DOS 32 and wbStego4.3 open steganography softwares.

A. *Solution Methodology*

The proposed system involves two software windows i.e. SNOW DOS 32 and wbStego4.3open. The user will be someone who is aware with the process of information hiding and will have adequate knowledge of steganography systems. The user first selects the plain text message from a file or enters text in specified area of software, another text to be used as the carrier (cover text). Then every tool will hide the message in the selected cover text and will procedure the stego text. Then create stego in various length of message and find out the moments which are shown in Fig. 2 and 3. After the comparison in between these values it has been observed that the system wbStego4.3open has minimum changes found for each order of moment (Fig. 4, Fig. 5), whereas the SNOW DOS 32 graph is decreasing for increase of embedding capacity.

III. EXPERIMENTAL RESULTS

The steganalyzer has been designed based on a training set and using various text steganographic tools. The steganographic tools used here *SNOW DOS 32 & wbStego4.3open*. In the experiments one cover and 30 input message were used for training and 20 cover text for testing. These experiments are performed using a large data set of text document obtained from publicly available websites. The data set is categorized with respect to different features of the text to determine their potential impact on steganalysis performance. Fig. 6 and Fig. 7 shows that the graphical representation of 2nd Order Moment of SNOW DOS 32 and wbStego4.3open. Here it has been observe that the graph SNOW is decreasing for high embedding where as the wbStego graph is increasing for high embedding. So it has proved that the performance and capasity of wbStego is better than SNOW.

IV. CONCLUSIONS

In this paper, text based steganalysis techniques of some module is tested based on moments and other similarity measure feature to evaluate what is the best. The plane text has been selected as an estimate of the cover-object. Next step is to use statistical, invariant and other similarity measure features to measure the distortion and to determine the presence of hidden information in a text. Results from moments with numerous text series showed that the proposed steganalysis algorithm provides significantly better analysis rates than existing ones. The author's future goal is to compare these tools with author's own generic module of steganography.

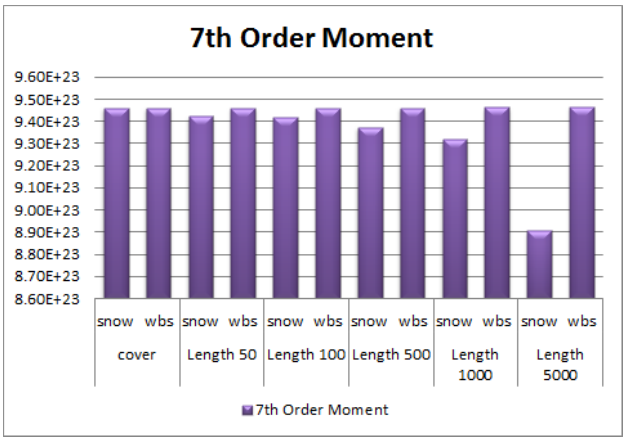


Figure 5: 7th Order Moment values of SNOW & wbStego4.3open.

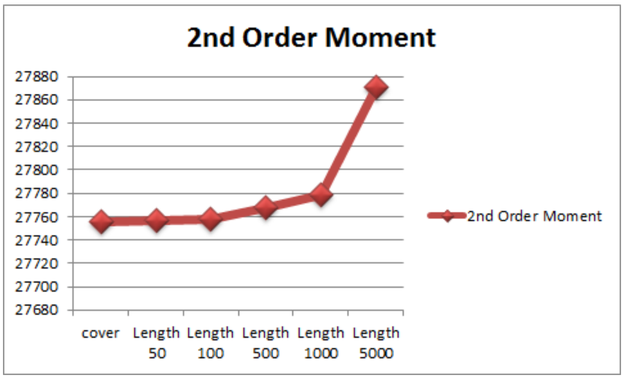


Figure 6: 2nd Order Moment graph of wbStego4.3open.

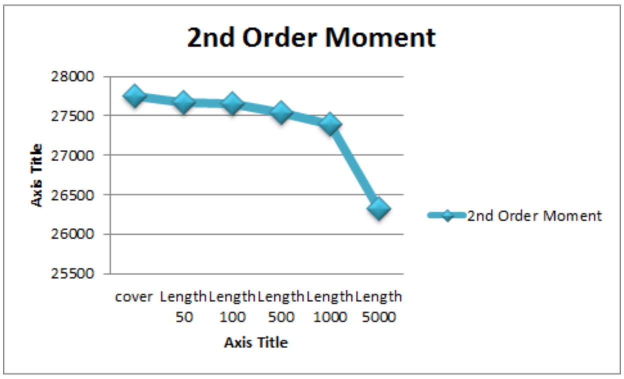


Figure 7: 2nd Order Moment graph of SNOW.

REFERENCES

[1] Fabien A.P. Petitcolas, Ross J. Anderson, Markus G. Kuhn: Information Hiding—A Survey, Proceedings of the IEEE, Vol. 87, No. 7, July 1999, pp. 1062-1078, ISSN 0018-9219.

[2] K. Bennett. Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text. Purdue University, CERIAS Tech. Report, 2004.

[3] Ross J. Anderson. and Fabien A.P.Petitcolas. On the limits of steganography. IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Copyright and Privacy Protection, 16:474–481, 1998.

[4] JHP Eloff T Mrkel and MS Olivier. An overview of image steganography. In Proceedings of the fifth annual Information Security South Africa Conference, South Africa, 2005.

[5] S.P.Mohanty. Digital watermarking: A tutorial review. International Journal of Digital Evidence, Fall 2003, 2003.

[6] N.F.Johnson. and S. Jajodia. Steganography: seeing the unseen. IEEE Computer, 16:26–34, 1998.

[7] Kran Bailey Kevin Curran. An evaluation of image based steganography methods. International Journal of Digital Evidence,Fall 2003, 2003.

[8] D. Kahn. The codebreakers - the comprehensive history of secret communication from ancient times to the internet. Scribner, 1996.

[9] Z. Duric N. F. Johnson and S. Jajodia. Information hiding: Steganography and digital watermarking - attacks and countermeasures. Kluwer Academic, 2001.

[10] S. Low N.F. Maxemchuk J.T. Brassil and L. O.Gorman. Electronic marking and identification techniques to discourage document copying. IEEE Journal on Selected Areas in Communications, 13:1495–1504, 1995.

[11] G. Doerr and J.L. Dugelay. Security pitfalls of framebyframe approaches to video watermarking. IEEE Transactions on Signal Processing, Supplement on Secure Media., 52:2955–2964, 2004.

[12] G. Doerr and J.L. Dugelay. A guide tour of video watermarking. Signal Processing: Image Communication., 18:263–282, 2003.

[13] Kran Bailey Kevin Curran. An evaluation of image based steganography methods. 1999.

[14] Krista Bennett (2004). " Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text". CERIAS TR 2004-13.

[15] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, “Information hiding - a survey”, Proceedings of the IEEE, Vol.87, No.7, pp.1062–1078, 1999.

[16] C. Kraetzer, J. Dittmann, “Pros and cons of melcepstrum based audio steganalysis using SVM classification”, The 9th International Workshop on Information Hiding, Saint Malo, France, pp.359–377, 2007.

[17] M.E. Choubassi, P. Moulin, “Noniterative algorithms for sensitivity analysis attacks”, IEEE Transactions on Information Forensics and Security, Vol.2, No.3, pp.113–126, 2007.

[18] O.H. Kocal, E. Avcibas, “Chaotic-type features for speech steganalysis”, IEEE Transactions on Information Forensics and Security, Vol.3, No.4, pp.651–661, 2008.

[19] Z.J. Wu, Y. Hu, X.X. Niu, H.X. Duan, X. Li, “Information hiding technique based speech secure communication over PSTN”, Chinese Journal of Electronics, Vol.15, No.1, pp.108–112, 2009.

[20] H. Shan, K. Darko, “An estimation attack on content-based video fingerprinting”, Transactions on Data Hiding and Multimedia Security II, Vol.4499, No.2007, pp.35–47, 2007.

[21] R. Bohme, “Weighted stego-image steganalysis for JPEG covers”, The 10th International Workshop on Information Hiding, Santa Barbara, California, USA, pp.178–194, 2008.

[22] L.J. Li, L.S. Huang, X.X. Zhao, W. Yang, Z.L. Chen, “A statistical attack on a kind of word-shift text-steganography”, The 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, China, pp.1503–1507, 2008.

[23] L.Y. Xiang, X.M. Sun, G. Luo, C. Gan, “Research on steganalysis for text steganography based on font format”, The 3rd International Symposium on Information Assurance and Security, Manchester, United Kingdom, pp.490–495, 2007.

[24] J.W. Huang, X.M. Sun, H. Huang, G. Luo, “Detection of hidden information in webpages based on randomness”, The 3rd International Symposium on Information Assurance and Security, Manchester, United kingdom, pp.447–452, 2007.

[25] H.J. Huang, X.M. Sun, Z.H. Li, G. Sun, “Detection of steganographic information in tags of webpage”, The 2nd International Conference on Scalable Information Systems, Brussels, Belgium, pp.325–328, 2007.

[26] H.J. Huang, S.H. Zhong, X.M. Sun, “Steganalysis of information hidden in webpage based on higher-order statistics”, Proceedings of the International Symposium on Electronic Commerce and Security, ISECS 2008, Guangzhou, China, pp.957–960, 2008.

[27] M. Chapman, G.I. Davida, M. Rennhard, “A practical and effective approach to large scale automated linguistic steganography”, The 4th International Conference on Information and Communications Security, Venice, Italy, pp.156–165, 2007.

[28] Z.L. Chen, L.S. Huang, Z.Z. Yu, W. Yang, L.J. Li, X.L. Zheng, X.X. Zhao, “Linguistic steganography detection using statistical characteristics of correlations between words”, The 11th International Workshop on Information Hiding, Darmstadt, Germany, pp.224–235, 2008.

[29] Z.L. Chen, L.S. Huang, Z.S. Yu, X.X. Zhao, X.L. Zheng, “Effective linguistic steganography detection”, The 8th IEEE International Conference on Computer and Information Technology Workshops, Sydney, Australia, pp.224–229, 2008.

[30] Z.L. Chen, L.S. Huang, Z.S. Yu, L.J. Li, W. Yang, “A statistical algorithm for linguistic steganography detection based on distribution of words”, The 3rd International Conference on Availability, Security, and Reliability, Barcelona, Spain, pp.558–563, 2008.

[31] C.M. Taskiran, U. Topkara, M. Topkara, E.J. Delp, “Attacks on lexical natural language steganography systems”, Proceedings of SPIE International Society for Optical Engineering, Society of Photo-Optical Instrumentation Engineers, San Jose, USA, pp.97–105, 2006.

[32] K. Bennett, “Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text”, Purdue University, Indiana, USA, 2004.

[33] YANG Hao and CAO Xianbin “ Linguistic Steganalysis Based on Meta Features and Immune Mechanism “Chinese Journal of Electronics,Vol.19, No.4, Oct. 2010

[34] Lingyun Xiang, Xingming Sun, Gang Luo, Can Gan. “Research on Steganalysis for Text Steganography Based on Font Format”, The Third International Symposium on Information

Assurance and Security (IAS 2007), Manchester, United Kingdom , August 2007.

[35] MOMENTS IN IMAGE PROCESSING Bob Bailey Nov. 2002

[36] Available online: http://home.tele2.at/wbailer/wbstego/wbs4devdoc . html

[37] Available online: http://www.darkside.com.au/snow/

[38] Indradip Banerjee, Souvik Bhattacharyya and Gautam Sanyal. "Novel text steganography through special code generation." In Proceedings of International Conference on Systemics,Cybernetics and Informatics (ICSCI-2011), Hyderabad,India., Jan 5-8, 2011.

[39] Indradip Banerjee, Souvik Bhattacharyya and Gautam Sanyal. "The text steganography using article mapping technique(AMT) and SSCE". Journal of Global Research in Computer Science, 2, April 2011.

[40] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal. Design and implementation of a secure text based steganography model. In 9th annual Conference on Security and Management (SAM) under The 2010 World Congress in Computer Science,Computer Engineering and Applied Computing(WorldComp 2010), Las Vegas,USA, July 12-15,2010.

[41] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal. Implementation of a novel text based steganography model. In National Conference on Computing and Systems (NACCS), Dept. of Computer Science, The University of Burdwan, Burdwan,India., Jan 29, 2010.

[42] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal. A novel approach of secure text based steganography model using word mapping method(WMM). International Journal of Computer and Information Engineering 4:2 2010 - World Academy of Science, Engineering and Technology (WASET), 4:96103, Spring 2010.

[43] Souvik Bhattacharyya, Indradip Banerjee, Arka Prokash Mazumdar and Gautam Sanyal. Text steganography using formatting character spacing. IJICS, 13, Decembar, 2010.

[44] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal. A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier. Journal of Global Research in Computer Science, 2, April 2011.

[45] Indradip Banerjee, Souvik Bhattacharyya and Gautam Sanyal. An Approach of Quantum Steganography through Special SSCE Code. International Journal of Computer and Information Engineering - World Academy of Science, Engineering and Technology (WASET), Issue 0080:2011, Article 175, Page: 939-946.

[46] Indradip Banerjee, Souvik Bhattacharyya and Gautam Sanyal. Text Steganography through Quantum Approach. In Journal on Wireless Networks And Computational Intelligence, Communications in Computer and Information Science, 2012, Volume 292, Part 7, 632-643, DOI: 10.1007/978-3-642-31686-9_74 Springer-Verlag Berlin Heidelberg 2012.

[47] Indradip Banerjee, Souvik Bhattacharyya and Gautam Sanyal. "A Procedure of Text Steganography Using Indian Regional Language" Journal on "I. J. Computer Network and Information Security, 2012, v. 8, p. 65-73" Published Online August 2012 in MECS.

Indradip Banerjee is a Research Scholar at National Institute of Technology, Durgapur, West Bengal, India. He received his MCA degree from IGNOU in 2009, PGDCA from IGNOU in 2008, MMM from Annamalai University in 2005 and BCA (Hons.) from The University of Burdwan in 2003. He is pursuing his PhD. in Engineering at Computer Science and Engineering Department, National Institute of Technology, Durgapur, West Bengal, India. His areas of interest are Steganography, Cryptography, Text Steganography, Image Steganography, Quantum Steganography and Steganalysis. He has published 16 research papers in International and National Journals / Conferences.

Souvik Bhattacharyya received his B.E. degree in Computer Science and Technology from B.E. College, Shibpur, India and M.Tech degree in Computer Science and Engineering from National Institute of Technology, Durgapur, India. Currently he is working as an Assistant Professor and In-Charge in Computer Science and Engineering Department at University Institute of Technology, The University of Burdwan. His areas of interest are Natural Language Processing, Network Security and Image Processing. He has published nearly 65 papers in International and National Journals / Conferences.

Gautam Sanyal has received his B.E and M.Tech degree National Institute of Technology (NIT), Durgapur, India. He has received Ph.D (Engg.) from Jadavpur University, Kolkata, India, in the area of Robot Vision. He possesses an experience of more than 25 years in the field of teaching and research. He has published nearly 150 papers in International and National Journals / Conferences. Two Ph.Ds (Engg) have already been awarded under his guidance. At present he is guiding six Ph.Ds scholars in the field of Steganography, Cellular Network, High Performance Computing and Computer Vision. He has guided over 10 PG and 100 UG thesis. His research interests include Natural Language Processing, Stochastic modeling of network traffic, High Performance Computing, Computer Vision. He is presently working as a Professor in the department of Computer Science and Engineering and also holding the post of Dean (Students' Welfare) at National Institute of Technology, Durgapur, India.