

Volume 2, No. 3, March 2011 Journal of Global Research in Computer Science

ISSN-2229-371X

RESEARCH PAPER

Available Online at www.jgrcs.info

Hiding Data in Text Through Changing in Alphabet Letter Patterns (CALP)

Souvik Bhattacharyya^{*1}, Pabak Indu², Sanjana Dutta³, Ayan Biswas⁴ and Gautam Sanyal⁵

*¹ Department of Computer Science and Engineering, University Institute of Technology The University of Burdwan, Burdwan, India.

souvik.bha@gmail.com¹

^{2,3,4} Department of Computer Science and Engineering, University Institute of Technology

The University of Burdwan, Burdwan, India.

pabakindu@yahoo.co.in², sanjana.dutta123@gmail.com³, destiny.ayan@gmail.com⁴

⁵ Department of Computer Science and Engineering, National Institute of Technology Durgapur, India.

nitgsanyal@gmail.com⁵

Abstract: Recent years have witnessed the rapid development of the Internet and telecommunication techniques But due to hostilities of environment over the internet, confidentiality of information have increased at phenomenal rate. Therefore to safeguard the information from attacks, number of data/information hiding methods have evolved. Steganography is an emerging area which is used for secured data transmission over any public media. Steganography is of Greek origin and means "Covered or hidden writing". Considerable amount of work has been carried out by different researchers on Steganography. In this paper the authors propose a novel text steganography method through changing the pattern of English alphabet letters. Considering the structure of English alphabets, secret message has been mapped through some little structural modification of some of the alphabets of the cover text .This approach uses the idea of structural and feature changing of the cover carrier which is not visibly distinguishable from the original to the human beings and may be modified for other India language also. This solution is independent of the nature of the data to be hidden and produces a stego text with minimum degradation. Quality of the stego text is analyzed by trade off between no of bits used for mapping. Efficiency of the proposed method is illustrated by exhaustive experimental results and comparisons.

Keywords: Steganography, Cover Text, Stego Text, CALP (Changing in Alphabet Letter Patterns), Pattern Change, Jaro-Winkler Distance.

INTRODUCTION

The technique of information hiding has been widely applied on various fields during the recent years [7] and the two major branches, viz. digital watermarking and steganography have been derived [9], [11]. Digital watermarking provides the protection of intellectual property, whereas steganography concerns privacy of information under surveillance. Steganalysis is the art of detecting any hidden message on the communication channel. If the existence of the hidden message is revealed, the goal of steganography is defeated. Steganography is an ancient art of conveying messages in a secret way that only the receiver knows the existence of the message [5]. The well-known steganographic methods include invisible ink, micro dot, covert channel, and spread spectrum communication. A famous illustration of modern day steganography is Simmons' Prisoners' Problem [1]. The term steganography is a Greek word means "covered writing". As the goal of steganography is to hide the presence of a message and to create a covert channel, it can be seen as the complement of cryptography, whose goal is to hide the content of a message. The message is hidden in another media such that the transmitted data will be meaningful and innocuous looking to everyone. Compared with cryptography attempting to conceal the content of the secret message, steganography conceals the very existence of that [8]. Fig 1 shows the framework of modern day steganography.

In steganography two aspects are usually addressed. First, the cover-media and stego media should appear identical

under all possible statistical attacks. Second, the embedding process should not degrade the media fidelity, that is, the difference between the stego media and the cover-media should be imperceptible to human perceptual system.



Figure 1: Frame work of modern day Steganography

Steganography works have been carried out on different transmission media like images, video, text, or audio [13].and receiver. If the public key of the receiver is known to the sender, the steganographic protocol is called public key steganography [4, 7]. Although all digital file formats can be used for steganography, but the image and audio files are more suitable because of their high degree of redundancy [21]. Fig. 2 below shows the different categories

of file formats that can be used for steganography techniques.



Figure 2: Types of Steganography

Among them image steganography is the most popular of the lot. In this method the secret message is embedded into an image as noise to it, which is nearly impossible to differentiate by human eyes [10, 12, 14]. In video steganography, same method may be used to embed a message [15, 20]. Audio steganography embeds the message into a cover audio file as noise at a frequency out of human hearing range [16]. One major category, perhaps the most difficult kind of steganography is text steganography or linguistic steganography [3]. The text steganography is a method of using written natural language to conceal a secret message as defined by Chapman et al. [13]. The advantage to prefer text steganography over other media is its smaller memory occupation and simpler communication. For a more thorough knowledge of steganography methodology the reader may see [10], [21]. Some Steganographic model with high security features has been presented in [25-31]. A block diagram of a generic text steganographic system is given in Fig. 3.



Figure 3: Generic form of Text Steganography

A block diagram of a generic form of text steganographic system is given in Fig. 3. A message is embedded in a carrier (cover text) through an embedding algorithm, with the help of a secret key. The resulting stego text is transmitted over a channel to the receiver where it is processed by the extraction algorithm using the same key. During transmission the stego text, it can be monitored by unauthenticated viewers who will only notice the transmission of an innocuous text without discovering the existence of the hidden message.

This paper has been organized as following sections:-Section II discusses about some of the related works done based on text steganography. Section III describes proposed text steganography method. Section IV describes the solution methodology. Section V describes different algorithms Section VI contains the analysis of the results and Section VII draws the conclusion.

RELATED WORKS ON TEXT STEGANOGRAPHY

Text steganography can be broadly divided into three types. They are format-based, random & statistical generations and Linguistic method shown in Figure 4. Most peoples have suggested various methods for hiding information in text in mentioned three categories. Some of the methods are discussed in this paper. Format-based methods use and change the formatting of the cover-text to hide the data. They don't change any words or sentences, so it does not harm the 'value' of the cover-text. A format-based text steganography method is open space method. In this method extra white spaces are added into the text to hide information. These white spaces can be added after end of each word, sentence or paragraph. A single space is interpreted as "0" and two consecutive spaces are interpreted as "1" [6]. Although a little amount of data can be hidden in a document, this method can be applied to almost all kinds of text without revealing the existence of the hidden data.



Figure 4: Types of Text Steganography

Another two format-based methods are word shifting and line shifting. In word shifting method, the horizontal alignments of some words are shifted by changing distances between words to embed information [18]. These changes are hard to interpret because varying distances between words are very common in documents. Another method of hiding information is, in manipulation of whitespaces between words and paragraph [23]. In line shifting method, vertical alignments of some lines of the text are shifted to create a unique hidden shape to embed a message in it [19]. Random and statistical generation methods are used to generate cover-text automatically according to the statistical properties of language. These methods use example grammars to produce cover-text in a certain natural language. A probabilistic context-free grammar (PCFG) is a commonly used language model where each transformation rule of a context-free grammar has a probability associated with it [2]. A PCFG can be used to generate word sequences by starting with the root node and recursively applying randomly chosen rules. The sentences are constructed according to the secret message to be hidden in it. The quality of the generated stego-message depends directly on the quality of the grammars used. Another approach to this type of method is to generate words having same statistical properties like word length and letter frequency of a word in the original message. The words generated are often without of any lexical value. The last category, the linguistic method considers the linguistic properties of the text to modify it. The method uses linguistic structure of the message as a place to hide information. Syntactic method is a linguistic steganography method where some punctuation signs like comma (,) and full-stop (.) are placed in proper places in the document to embed a data. This method needs proper identification of places where the signs can be inserted. Another linguistic steganography method is semantic method. In this method the synonym of words for some preselected are used. The words are replaced by their synonyms to hide information in it [17]. Except the above mentioned

methods, there are some other methods proposed for text steganography, such as feature coding, text steganography by specific characters in words, abbreviations etc. [22] or by changing words spelling [24].

PROPOSED METHOD FOR TEXT STEGANOGRAPHY (CALP)

In this paper, a new method for text steganography for English language is proposed. In this method cover text and secret message is generated by the user. Stego text is formed by mapping the binary sequence of the secret message through texture/pattern changes of some alphabets of the cover text. Figure 5 and 6 below respectively shows the mapping sequence for embedding 0s and 1s through the following pattern changes of the following alphabets of the cover text. These pattern changes have been incorporated using some unused symbols of the ASCII chart.







Figure 6: Mapping sequence for embedding '1'

SOLUTION METHODOLOGY

The proposed system consists of the following two windows, one for the cover text generation and the other for the secret message generation. The user will be someone who is familiar with the process of information hiding and will have the knowledge of steganography systems. The user should be able to form a plain text as secret message, another text needs to be formed for use as carrier (cover text).Finally the proposed embedding method will be used to hide the secret message in cover text to form the stego text.The user at the receiver side should be able to extract the secret message from the stego text with the help of different reverse process. Figure 7 shows the corresponding GUI for the proposed text steganography system





ALGORITHMS

In this section algorithmic process for embedding and extraction methodology has been discussed. Figure. 8 show the block diagram of the proposed steganographic system. This input message is first converted into bits according to their ASCII values. Then the bit is embedded into the cover text according to the methods mentioned earlier and thus stego text is generated.



Figure 8: Proposed Algorithm for Steganographic Model

A. Algorithm Stego Text formation

Let COVER be the cover text and STEGO be the stego text and MSG is the binary string of the secret message and N is the no of elements in the MSG. Initially COVER and STEGO are the same. Set two counters i and j initialize to 1. Take an array arr to keep the embeeding positions.

Step 1: Generate an appropriate COVER consisting of 'A' or 'a' or 'c' and 'i' or 'j'. Let k be the size of the COVER.

or

Copy the contents of the COVER into STEGO.

Step 2: For i=1 to k

Step 3: if (COVER (i) =='a' or 'A' or 'c') then go to step4 else if(COVER(i) =='i' or 'j') then go to step6.

Step 4: if (MSG(j) =='1') then put STEGO(i) = 2

Step 5: End of Step4.

Step 6:if (MSG(j) == 0) then put STEGO(i) = 0 or 0. Step 7: End of Step 6.

Step 8: Insert i into array arr.

Step 9: Increment j.

Step 10:if (j<N) Then go to Step3 Else go to Step 11.

Step 11: End of if statement.

Step 12: End of for.

Step 13: End.

B. Algorithm for Message Extracting

Let STEGO is the stego text and MSG is the binary string of the secret message and N is the no. of elements in the MSG and arr is array containing the position of embedding and i be the index of the array arr and j=1.

Step 1: For i=1 to N Step 2: Get the text STEGO.

Step 3: if (STEGO (i)== 2 or A or C) then MSG(j)=1 Else go to step4.

Step 4: if (STEGO(i)== ' i ' or ' j ') then MSG(j)=0. Step 5: End of for. Step 6: End.

ANALYSIS OF THE RESULTS

There are mainly three aspects that should be taken into account when discussing the results of the proposed method of text steganography. They are security, capacity and robustness. The authors simulated the proposed system and the results are shown in the figures 9, 10, and 11 respectively. This method satisfies both security aspects and hiding capacity requirements. It generates the stego text with minimum degradation which is not very revealing to people about the existence of any hidden data, maintaining its security to the eavesdroppers. Although the embedding capacity of the proposed method depends upon the cover text structure but the embedding capacity can be maximized by incorporating more no of alphabets through minor pattern changes for mapping 0s and 1s.

The achievement of independence was of utmost importance to us The implications of subservience to another power remain as abhorrent today in this area of economic rather than military domination. Globalization, which means integration with the world economy, brings the influence of external forces into our society. Some experts may point out that these are economic or trade or market forces and they have beneficial influence in terms of developing our 'core competencies' in areas in which we have 'comparative advantage' advantage'. We also share the view that competition , both internally and with other global players would be useful to make the country efficient and strong. But we would also like to point out that developed co untries have set up several non-tariff barriers which strike at the roots of ideal competition based on 'market' forces. These are mostly aimed at denving opportunities to other countries to reach a developed status. Even when our country prepares to cope with a set of barriers introduced by these developed countries, either through their own laws or through multilateral treaties, a new set of complex barriers crops up. Even a simple analysis of many of these international or global transactions indicates a much deeper fact: the continuous process of domination over others by a few nations.

Figure 9: Cover Text

📃 secret.txt - Notepad

File Edit Format View Help

God is great



The achievement of independence was of utmost importance to us. The implications of subservience to another power remain as abhorent today in this area of economic rather than military domination.Globalization,which means integration with the world economy, brings the influence of external forces into our society. Some experts may point out that these are economic or trade or market forces and they have beneficial influence in terms of developing our 'core competencies' in areas in which we have 'comparative advantage'. We also share the view that competition, both internally and with other global players would be useful to make the country efficient and strong. But we would also like to point out that developed countries have set up several non-tariff barriers which strike at the roots of ideal competition based on 'market' forces. These are mostly aimed at denying opportunities to other countries to reach a developed status. Even when our country prepares to cope with a set of barriers introduced by these developed countries, either through their own laws or through multilateral treaties, a new set of complex barriers crops up . Even a simple analysis of many of these international or global transactions indicates a much deeper fact: the continuous process of domination over others by a few nations. Figure 11: Stego Text

Similarity Measure of the Cover Text and Stego Text through Correlation

The most familiar measure of dependence between two quantities is the Pearson product-moment correlation coefficient [32], or "Pearson's correlation." It is obtained by dividing the covariance of the two variables by the product of their standard deviations. Karl Pearson developed the coefficient from a similar but slightly different idea by Francis Galton. The Pearson correlation is +1 in the case of perfect positive (increasing) linear relationship а (correlation), -1 in the case of a perfect decreasing (negative) linear relationship (anti correlation), and some value between -1 and 1 in all other cases, indicating the degree of linear dependence between the variables. As it approaches zero there is less of a relationship (closer to uncorrelated). The closer the coefficient is to either -1 or 1, the stronger the correlation between the variables. If the variables are independent, Pearson's correlation coefficient is 0, but the converse is not true because the correlation coefficient detects only linear dependencies between two variables.

If we have a series of n measurements of X and Y written as x_i and y_i where i = 1, 2, ..., n then the sample correlation coefficient can be used in Pearson correlation r between X and Y. The sample correlation coefficient is written as

$$r_{xy} = \frac{\sum_{i=1}^{n} (x_i - \bar{x})(y_i - \bar{y})}{(n-1)s_x s_y}$$

where \bar{x} and \bar{y} are the sample means of X and Y, s_x and s_y are the sample standard deviations of X and Y.

Similarity Measure of the Cover Text and Stego Text through Jaro Winkler Distance

For comparing the similarity between cover text and the stego text, the Jaro-Winkler distance for measuring similarity between two strings has been computed. The Jaro-Winkler distance [35] is a measure of similarity between two strings. It is a variant of the Jaro distance metric [33], [34] and mainly used in the area of record linkage (duplicate detection). The higher the Jaro-Winkler distance for two strings is, the more similar the strings are. The score is normalized such that 0 equates to no similarity and 1 is an exact match. The Jaro distance metric states that given two strings s_1 and s_2 their distance d_j is $d_j = \frac{1}{3} \left[\frac{m}{|s_1|} + \frac{m-t}{m} \right]$, where *m* is the number of

matching characters and t is the number of transpositions. Two characters from s_1 and s_2 respectively are considered matching only if they are not farther $\frac{\max \left[\frac{s_1}{2} \right]^{-1}}{2} = 1$. Each character of s_1 is compared than L with all its matching characters in s_2 . The number of matching (but different sequence order) characters divided by two defines the number of transpositions. Figure12 below shows the Correlation coefficient and Jaro score for various size of cover text along with various size of the secret message of the proposed CALP method.

Secret Message	Cover Test Size	Correlation-	Jaro-
Size	(in characters)	coefficient	Score
(in characters)			
12	1312	0.721635	0.943598
12	1861	0.775256	0.956296
12	2623	0.824689	0.967976
12	1587	0.852256	0.953733
14	1312	0.783506	0.946032
14	1861	0.778333	0.959431
14	2623	0.813037	0.966196
14	1587	0.883468	0.951209
13	1587	0.835731	0.950789
13	2623	0.817092	0.966196
13	1312	0.712223	0.940041
13	1861	0.766338	0.954147

Figure 12: CALP parameters

CONCLUDING REMARKS

In this paper the authors presented a novel approach of English text steganography method .Stego text is generated by mapping the binary sequence of the secret message through texture/pattern changes of some alphabets of the cover text in order to achieve high level of security. From figure 12 it has been observed that CALP method generates the stego text with minimum or zero degradation as both the Jaro score and Correlation-coefficient value is very high. This property also enables the method to avoid the steganalysis. The proposed steganography technique through texture/pattern changing is a new approach for the English steganography and this methodology can be extended to any Indian language also.

REFERENCES

- Gustavus J. Simmons, "The Prisoners' Problem and the Subliminal Channel", in Proceedings of CRYPTO '83, pp 51-67. Plenum Press (1984).
- [2] P. Wayner, "Strong Theoretical Steganography", Cryptologia, XIX(3), July 1995, pp. 285-299.
- [3] J.T. Brassil, S. Low, N.F. Maxemchuk, and L. O'Gorman, "Electronic Marking and Identification Techniques to Discourage Document Copying", *IEEE Journal on Selected Areas in Communications*, vol. 13, Issue. 8, October 1995, pp. 1495-1504.
- [4] "Stretching the Limits of Steganography", RJ Anderson, in Information Hiding, Springer Lecture Notes in Computer Science v 1174 (1996) pp 39-48.
- [5] Kahn, The Codebreakers the comprehensive history of secret communication from ancient times to the Internet, Scribner, New York (1996).
- [6] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", *IBM Systems Journal*, vol. 35, Issues 3&4, 1996, pp. 313-336.
- [7] Scott Craver, "On Public-key Steganography in the Presence of an Active Warden," in Proceedings of 2nd International Workshop on Information Hiding, April 1998, Portland, Oregon, USA. pp. 355 - 368.
- [8] 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 & Privacy Protection, vol. 16 no. 4, pp 474-481, May 1998.
- [9] N. F. Johnson and S. Jajodia, "Steganography: seeing the unseen," IEEE Computer., Feb., 26-34 (1998).
- [10] L. M. Marvel, C. G. Boncelet, Jr. and C. T. Retter, "Spread spectrum image steganography," IEEE Trans. on Image Processing, 8(8), 1075-1083 (1999).
- [11] Digital Watermarking : A Tutorial Review S.P.Mohanty ,1999.
- [12] Analysis of LSB Based Image Steganography Techniques ,R. Chandramouli, Nasir Memon, Proc. IEEE ICIP, 2001.
- [13] M.Chapman, G. Davida, and M. Rennhard, "A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography", *Proceedings of the Information Security Conference*, October 2001, pp. 156-165.
- [14] An Evaluation of Image Based Steganography Methods, Kevin Curran, Kran Bailey, International Journal of Digital Evidence, Fall 2003.
- [15]G. Doërr and J.L. Dugelay, "A Guide Tour of Video Watermarking", *Signal Processing: Image Communication*, vol. 18, Issue 4, 2003, pp. 263-282.
- [16] K. Gopalan, "Audio steganography using bit modification", Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '03), vol. 2, 6-10 April 2003, pp. 421-424.
- [17] M. Niimi, S. Minewaki, H. Noda, and E.Kawaguchi, "A Framework of Text-based

Steganography Using SD-Form Semantics Model", Pacific Rim Workshop on Digital Steganography 2003, Kyushu Institute of Technology, Kitakyushu, Japan, July 3-4, 2003.

- [18] Y. Kim, K. Moon, and I. Oh, "A Text Watermarking Algorithm based on Word Classification and Inter-word Space Statistics", Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR'03), 2003, pp. 775-779.
- [19] A.M. Alattar and O.M. Alattar, "Watermarking electronic text documents containing justified paragraphs and irregular line spacing ", Proceedings of SPIE - Volume5306, Security, Steganography, and Watermarking of Multimedia Contents VI, June 2004, pp- 685-695.
- [20] G. Doërr and J.L. Dugelay, "Security Pitfalls of Frameby-Frame Approaches to Video Watermarking", IEEE Transactions on Signal Processing, Supplement on Secure Media, vol. 52, Issue 10, 2004, pp. 2955-2964.
- [21] T Mrkel, JHP Eloff and MS Olivier ."An Overview of Image Steganography ,"in proceedings of the fifth annual Information Security South Africa Conference,2005
- [22] M.H. Shirali-Shahreza and M. Shirali-Shahreza, "Text Steganography in Chat", Proceedings of the Third IEEE/IFIP International Conference in Central Asia on Internet the Next Generation of Mobile, Wireless and Optical Communications Networks (ICI 2007), Tashkent, Uzbekistan, September 26-28, 2007.
- [23] L.Y. Por and B. Delina, "Information Hiding: A New Approach in Text Steganography", 7th WSEAS International Conference on Applied Computer & Applied Computational Science, April 2008, pp- 689-695.
- [24] MohammadShirali-Shahreza: "Text Steganography by Changing Words Spelling" at ICACT 2008.
- [25] "Study of Secure Steganography model" by Souvik Bhattacharyya and Gautam Sanyal at the proceedings of "International Conference on Advanced Computing & Communication Technologies (ICACCT-2008), Nov, 2008, Panipat, India"
- [26] "An Image based Steganography model for promoting Global Cyber Security" by Souvik Bhattacharyya and Gautam Sanyal at the proceedings of "International Conference on Systemics, Cybernetics and Informatics (ICSCI-2009), Jan, 09, Hyderabad, India."
- [27] "Implementation and Design of an Image based Steganographic model" by Souvik Bhattacharyya and Gautam Sanyal at the proceedings of " IEEE International Advance Computing Conference "(IACC-2009)"
- [28] A Novel Approach to Develop a Secure Image based Steganographic Model using Integer Wavelet Transform" at the proceedings of International Conference on Recent Trends in Information, Telecommunication and Computing (ITC 2010)" by Souvik Bhattacharyya, Avinash Prasad Kshitij

and Gautam Sanyal. (Indexed by IEEE Computer Society).

- [29] A Steganographic Method for Images using Pixel Intensity Value (PIV))" by Souvik Bhattacharyya and Gautam Sanyal at the proceedings of National Conference on Computing & Systems 2010 held at The University of Burdwan in January 2010.
- [30] "Hiding Data in Images Using Pixel Mapping Method (PMM) by Souvik Bhattacharvva and Gautam Sanyal accepted as a regular research paper at SAM'10 - 9th annual Conference on Security and Management under The 2010 World Congress in Computer Science, Computer Engineering, and Applied Computing to be held on July 12-15, 2010, USA (The proceedings will be indexed in Inspec / IET / The Institute for Engineering and Technology; DBLP / Computer Science Bibliography, and others.)
- [31] "Design and implementation of a secure text based steganography model" by Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal at the Proceedings of 9th annual Conference on Security and Management (SAM) under The 2010 World Congress Computer Science,Computer in Engineering and Applied Computing(WorldComp 2010), LasVegas, USA, July 12-15, 2010.
- [32] S. Dowdy and S. Wearden. Statistics for research. Wiley. ISBN 0471086029, page 230, 1983.
- [33] M. A. Jaro. Advances in record linking methodology as applied to the 1985 census of tampa florida. Journal of the American Statistical Society. 84:414-420, 1989.
- [34] M. A. Jaro. Probabilistic linkage of large public health data file. Statistics in Medicine 14 (5-7)., pages 491-498, 1995.
- [35] W. E. Winkler. The state of record linkage and current research problems. Statistics of Income Division, Internal Revenue Service Publication R99/04., 1999.

About the authors



Souvik Bhattacharyya received his B.E. degree in Computer Science and Technology from B.E. College, Shibpur, India, presently known as Bengal Engineering and Science University (BESU) and M.Tech degree in Computer

Science and Engineering from National Institute of Technology, Durgapur, India. Currently he is working as an Assistant Professor in Computer Science and Engineering Department at University Institute of Technology, The University of Burdwan. He has a good no of research publication in his credit. His areas of interest are Natural Language Processing, Network Security and Image Processing.



Sanjana Dutta is currently doing her B.E in Information Technology at University Institute Of Technology, The University of Burdwan.She is a final year student of this

course and her areas of interest are E-Commerce, Database and Client Server Technology.



Ayan Biswas is currently doing her B.E in Information Technology at University Institute Of Technology, The University of Burdwan .He is a final year student of this course and

hirs areas of interest are Database, Web Technology and Computer Network.



Pabak Indu is currently doing her B.E in Information Technology at University Institute Of Technology, The University of Burdwan .He is a final year student of this course and

hirs areas of interest are Database, Web Technology and Computer Network.



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 50 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.