# COMPARATIVE STUDY ON DATA ENCRYPTION STANDARD USING DIFFERENTIAL CRYPTANALYSIS AND LINEAR CRYPTANALYSIS

Rajashekarappa[1], K M Sunjiv Soyjaudah[2], and Sumithra Devi K A[3]
[1]Department of Computer Science and Engineering, JSS Academy of Technical Education, Vacoas, Mauritius. (Research Scholar, Jain University, Bangalore, India)
[2]Department of Electrical & Electronic Engg., University of Mauritius, Reduit, Mauritius.
[3]Department of Master of Computer Applications, R V College of Engg,. Bangalore, India.

***ABSTRACT***

*This paper presents an approach for the comparative study on Data Encryption Standard (DES) using Differential Cryptanalysis and Linear cryptanalysis. In this paper, cipher text only attack is adopted and varieties of optimum keys are generated based on the cost function values. The goal of this paper is two fold. First we want to make a study about how evolutionary computation techniques can efficiently solve the NP-Hard combinatorial problem. For achieving this goal we test several evolutionary computation techniques for the cryptanalysis of data encryption standard problem (DES). Second was a comparison between Differential Cryptanalysis and Linear cryptanalysis were made in order to investigate the performance for the cryptanalysis on DES. The methods were tested and extensive computational results shown in this paper. For most of its life, the prime concern with DES has been its vulnerability to brute-force attack because of its relatively short (56 bits) key length. However, there has also been interest in finding cryptanalytic attacks on DES. With the increasing popularity of block ciphers with longer key lengths, including triple DES, brute-force attacks have become increasingly impractical. Thus, there has been increased emphasis on cryptanalytic attacks on DES and other symmetric block ciphers. In this paper, we provide a brief overview of the two most powerful and promising approaches: differential cryptanalysis and linear cryptanalysis.*

***KEYWORDS:*** *Cryptanalysis, Data Encryption Standard (DES), Plain text, Cipher text, Cipher text attack.*

## I. INTRODUCTION

The process of studying methods of encryption to obtain information from encrypted data without knowing the secret key is called cryptanalysis. It is usually a deep analysis and attacking of an encryption method to find the secret key. The cryptanalysis of data encryption standard can be formulated as NP-Hard combinatorial problem. Solving such problems requires effort (e.g., time and/or memory requirement) which increases with the size of the problem. Two important methods of cryptanalysis are differential cryptanalysis and linear cryptanalysis. DES has been shown to be highly resistant to these two types of attack.

Differential cryptanalysis [1] and linear cryptanalysis have shown to be two of the most important techniques in the analysis of symmetric-key cryptographic primitives. For block ciphers, differential cryptanalysis analyzes how input differences in the plaintext lead to output differences in the ciphertext. Linear cryptanalysis studies probabilistic linear relations between plaintext, ciphertext and key. If a cipher behaves differently from a random cipher for differential or linear cryptanalysis, this can be used to build a distinguisher or even a key-recovery attack.

The aim of these techniques to find sufficient "good" solution efficiently with the characteristics of the problem, instead of the global optimum solution, and thus it also provides attractive alternative for the large scale applications. These nontraditional optimization techniques demonstrate good potential when applied in the field of cryptanalysis. The objective of the study is to determine the efficiency and accuracy of differential cryptanalysis and linear cryptanalysis for the DES[2,3]. To compare the relative performance of differential cryptanalysis and linear cryptanalysis.
The rest of the paper is organized as follows: Section 2 presents the literature review. Section 3 gives a brief overview of Comparative Study on DES Using Differential Cryptanalysis and Linear Cryptanalysis. Experimental results are discussed in Section 4. Section 5 concludes the paper and Future works.

## II. RELATED WORK

The proposed work will require an in depth understanding of the area of cryptography and enable the development of general as well as specific algorithms for cryptanalysis [1]. Moreover, the enciphering algorithms developed in this work will find many real time applications in military, banking and other sectors where secure transmission is essential. A cipher takes a message text and some secret keying data (known as the key) as its input and produces an encrypted version of the original message, (known as the cipher text). An attack on a cipher can make use of the cipher text alone or it can make use of some plaintext and its corresponding cipher text (referred to as a known plaintext attack) (Andrew John Clark, 1998). Cryptanalysis is the process of recovering the plaintext and/or key from a cipher. Many cryptographic systems have a finite key space and, hence, are vulnerable to an exhaustive key search attack. Yet, these systems remain secure from such an attack because the size of the key space is such that the time and resources required for a search are prohibitive. A Linear Cryptanalysis Method for DES Cipher was explained by Matsui in 1993[4]. Differential cryptanalysis was not reported in the open literature until 1990. The first published effort appears to have been the cryptanalysis of a block cipher called FEAL by Murphy. This was followed by a number of papers by Biham and Shamir, who demonstrated this form of attack on a variety of encryption algorithms and hash functions; their results are summarized in this paper [2]. The most publicized results for this approach have been those that have application to DES.
Differential cryptanalysis is the first published attack that is capable of breaking DES in less than 255 complexity [5]. The scheme, as reported in Biham [2], can successfully cryptanalyze DES with an effort on the order of 247 encryptions, requiring 247 chosen plaintexts. Although 247 is certainly significantly less than 255 the need for the adversary to find 247 chosen plaintexts makes this attack of only theoretical interest [5]. In [17] we proposed "Heuristic Search Procedures for Cryptanalysis and Development of Enhanced Cryptographic Techniques". To implement the proposed Tabu search, Genetic, and Simulated Annealing algorithms firstly by utilising cipher text as well as some plain text and secondly by using only the cipher text to retrieve the original data. The cryptanalysis of simplified data encryption standard can be formulated as NP-Hard combinatorial problem. A simple heuristic for the attack of known ciphertext with a pair of them has been developed to retrieve the plaintext to almost 90% accuracy for a SDES 10-bit key. Although differential cryptanalysis is a powerful tool, it does not do very well against DES. The reason, according to a member of the IBM team that designed DES [3], is that differential cryptanalysis was known to the team as early as 1974. The need to strengthen DES against attacks using differential cryptanalysis played a large part in the design of the S-boxes and the permutation P. As evidence of the impact of these changes, consider these comparable results reported by Biham [2]. Differential cryptanalysis of an eight-round LUCIFER algorithm requires only 256 chosen plaintexts, whereas an attack on an eight-round version of DES requires 214 chosen plaintexts [6]. A.Zugaj, K. Górski, Z. Kotulski, A. Paszkiewicz, J. Szczepański,"New constructions in linear cryptanalysis of block ciphers", ACS'2000, October [16]. The differential cryptanalysis attack is complex; [2] provides a complete description. The rationale behind differential cryptanalysis is to observe the behavior of pairs of text blocks evolving along each round of the cipher, instead of observing the evolution of a single text block. Here, we provide a brief overview so that we can get the flavor of the attack [6, 7, 8, 9].

# III. COMPARATIVE STUDY ON DES USING DIFFERENTIAL CRYPTANALYSIS AND LINEAR CRYPTANALYSIS

In this paper for most of its life, the prime concern with DES has been its vulnerability to brute-force attack because of its relatively short (56 bits) key length. However, there has also been interest in finding cryptanalytic attacks on DES. With the increasing popularity of block ciphers with longer key lengths, including triple DES, brute-force attacks have become increasingly impractical. Thus, there has been increased emphasis on cryptanalytic attacks on DES and other symmetric block ciphers. In this section, we provide a brief overview of the two most powerful and promising approaches: differential cryptanalysis and linear cryptanalysis [8,13].
The Differential cryptanalysis one of the most significant advances in cryptanalysis in recent years is differential cryptanalysis. In this section, we discuss the technique and its applicability to DES [15].

## 2.1. Differential Cryptanalysis Attack

The differential cryptanalysis attack is complex; [2] provides a complete description. The rationale behind differential cryptanalysis is to observe the behavior of pairs of text blocks evolving along each round of the cipher, instead of observing the evolution of a single text block. Here, we provide a brief overview so that we can get the flavor of the attack. We begin with a change in notation for DES. Consider the original plaintext block m to consist of two halves m0,m1. Each round of DES maps the right-hand input into the left-hand output and sets the right-hand output to be a function of the left-hand input and the subkey for this round. So, at each round, only one new 32-bit block is created. If we label each new block m1($2 \leq i \leq 17$), then the intermediate message halves are related as follows:

$m_{i+1} = m_{i-1} \oplus f(m_i, K_i)$, i = 1, 2, ..., 16

In differential cryptanalysis, we start with two messages, m and m', with a known XOR difference $\Delta m = m \oplus m'$, and consider the difference between the intermediate message halves: $mi = mi \oplus mi'$ Then we have:

$$m_{i+1} = m_{i+1} \oplus m'_{i+1}$$
$$= [m_{i-1} \oplus f(m_i, K_i)] \oplus [m'_{i-1} \oplus f(m'_i, K_i)]$$
$$= \Delta m_{i-1} \oplus [f(m_i, K_i) \oplus f(m'_i, K_i)]$$

Now, suppose that many pairs of inputs to f with the same difference yield the same output difference if the same subkey is used. To put this more precisely, let us say that X may cause Y with probability p, if for a fraction p of the pairs in which the input XOR is X, the output XOR equals Y. We want to suppose that there are a number of values of X that have high probability of causing a particular output difference. Therefore, if we know $\Delta mi-1$ and $\Delta mi$ with high probability, then we know $\Delta mi+1$ with high probability. Furthermore, if a number of such differences are determined, it is feasible to determine the subkey used in the function f[18,19].
The overall strategy of differential cryptanalysis is based on these considerations for a single round. The procedure is to begin with two plaintext messages *m* and *m*' with a given difference and trace through a probable pattern of differences after each round to yield a probable difference for the ciphertext. Actually, there are two probable patterns of differences for the two 32-bit halves: ($\Delta m17 || m16$). Next, we submit *m* and *m*' for encryption to determine the actual difference under the unknown key and compare the result to the probable difference. If there is a match,
$E(K, m) \oplus E(K, m') = (\Delta m17 || m16)$

then we suspect that all the probable patterns at all the intermediate rounds are correct. With that assumption, we can make some deductions about the key bits. This procedure must be repeated many times to determine all the key bits [20,21,22].
Figure 1 illustrates the propagation of differences through three rounds of DES. The probabilities shown on the right refer to the probability that a given set of intermediate differences will appear as a function of the input differences. Overall, after three rounds the probability that the output difference is as shown is equal to 0.25 x 1 x 0.25 = 0.0625.

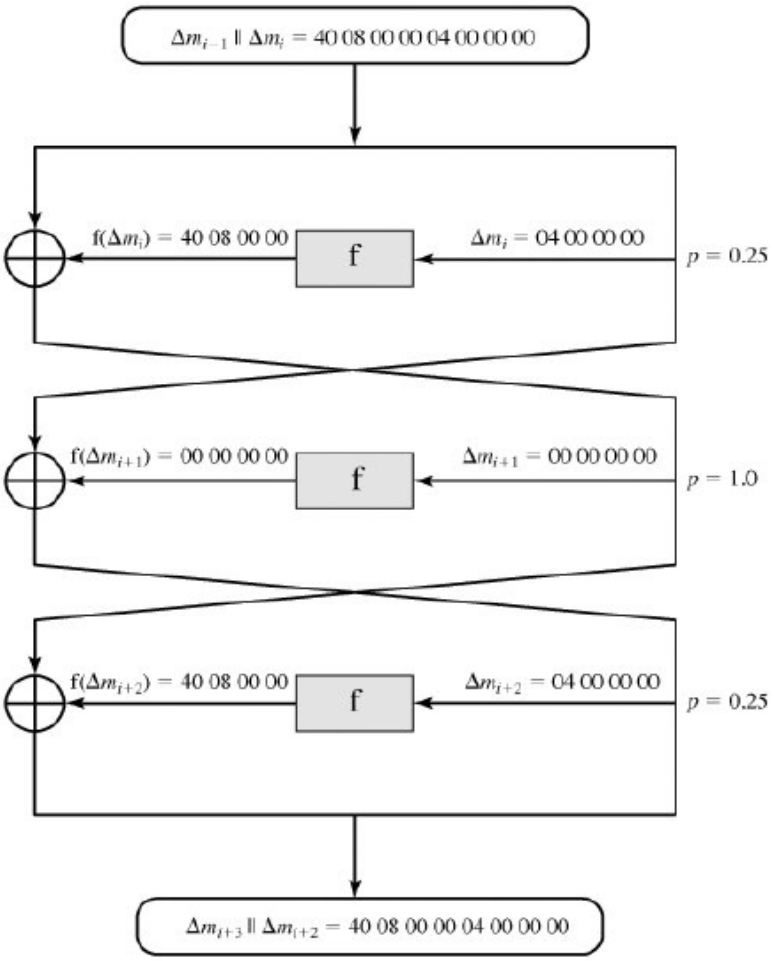


**Figure 1.** Differential Propagation through Three Round of DES (numbers in hexadecimal)

## 2.2. Linear Cryptanalysis

A more recent development is linear cryptanalysis, described by Matsui [4]. This attack is based on finding linear approximations to describe the transformations performed in DES. This method can find a DES key given 243 known plaintexts, as compared to 247 chosen plaintexts for differential cryptanalysis [13]. Although this is a minor improvement, because it may be easier to acquire known plaintext rather than chosen plaintext, it still leaves linear cryptanalysis infeasible as an attack on DES. So far, little work has been done by other groups to validate the linear cryptanalytic approach [12].

We now give a brief summary of the principle on which linear cryptanalysis is based. For a cipher with n-bit plaintext and ciphertext blocks and an *m*-bit key, let the plaintext block be labeled P[1], ... P[*n*], the cipher text block C[1], ... C[*n*], and the key K[1], ... K[*m*]. Then define
$A[i, j, ..., k] = A[i] \oplus A[j] \oplus ... \oplus A[k]$

The objective of linear cryptanalysis is to find an effective *linear* equation of the form:

$P[\alpha 1, \alpha 2, ..., \alpha a] \oplus C[\beta 1, \beta 2, ..., \beta b] = K[\gamma 1, \gamma 2, ..., \gamma c]$

(where $x = 0$ or 1; $1 \leq a, b \leq n$, $1 \leq c \leq m$, and where the α, β and γ terms represent fixed, unique bit locations) that holds with probability $p \neq 0.5$. The further $p$ is from 0.5, the more effective the equation. Once a proposed relation is determined, the procedure is to compute the results of the left hand side of the preceding equation for a large number of plaintext-ciphertext pairs. If the result is 0 more than half the time, assume $K[\gamma 1, \gamma 2, ..., \gamma c] = 0$. If it is 1 most of the time, assume $K[\gamma 1, \gamma 2, ..., \gamma c] = 1$. This gives us a linear equation on the key bits. Try to get more such relations so that we can solve for the key bits. Because we are dealing with linear equations, the problem can be approached one round of the cipher at a time, with the results combined [9,10,11].

## IV. EXPERIMENTAL RESULT

In this paper the number of experiments is carried out to outline the effectiveness of Comparative study on DES using Differential Cryptanalysis and Linear Cryptanalysis.

**MATLAB 7 Setup for experiments as follows**:
The experiments were implemented in MATLAB 7 on a Pentium IV(1.83 Ghtz). Experimental results obtained from these algorithms were generated with 200 runs per data point e.g. twenty different messages were created for all the algorithms and each algorithm was run 80 times per message. The best result for each message was averaged to produce data point.
The Differential Cryptanalysis and Linear Cryptanalysis is coded in MATLAB 7, and tested on more than 100 benchmark data sets adapted. We consider 30 different sets of distinct known plaintexts with different secret keys. In each experiment the behavior of the statistic test is studied for the right key and also for one wrong key. As predicted by the theoretical model, when more than $2^{30.2}$ distinct known plaintexts are used, the correct key is very likely to pass the test, while the wrong keys would fail. Access to the full codebook leads to the key recovery with negligible error probability. When using $2^{28}$ distinct known plaintexts, the right key survives with high probability. Table. 1 shows the number of bits recovered from the key using Linear cryptanalysis and differential cryptanalysis. As comparatively Differential Cryptanalysis is better than Linear Cryptanalysis of DES.

**Table. 1** The number of bits recovered from the key using Linear cryptanalysis and differential cryptanalysis.

| Amount of Cipertext | Linear Cryptanalysis | | Differential Cryptanalysis | |
|---|---|---|---|---|
| | Time(Minute) | Number of bits matched in the Key | Time(Minute) | Number of bits matched in the Key |
| **100** | 60 | 6 | 30 | 5 |
| **200** | 55 | 2 | 26 | 4 |
| **300** | 51.3 | 8 | 24 | 7 |
| **400** | 47.1 | 6 | 22 | 6 |
| **500** | 44 | 8 | 20 | 7 |
| **600** | 40 | 9 | 18.5 | 8 |
| **700** | 30 | 4 | 15 | 7 |
| **800** | 28.5 | 2 | 16 | 6 |
| **900** | 25 | 9 | 12 | 8 |
| **1000** | 20 | 7 | 10 | 9 |

## V. CONCLUSIONS

In this paper has demonstrated that the differential cryptanalysis and linear cryptanalysis are ideally suited for the cryptanalysis of Data Encryption Standard. Thus these techniques offer a lot of promises for attacks of the ciphers. The time complexity of the proposed approach has been reduced drastically when compared to the linear cryptanalysis. Experimental results demonstrate good performance for differential cryptanalysis than linear cryptanalysis few parameters need to be tuned for the best possible performance. Though DES is a simple encryption algorithm, this is a promising method and can be adopted to handle other complex block ciphers like DES and AES. The cost function values used here can be applied for other block ciphers also.

## VI. FUTURE ENHANCEMENT

This is the most promising method and can be used for handling other complex block ciphers like DES, AES and TEN in future work.

The cost function values used here can be applied for other block ciphers also.

## REFERENCES

[1]. Rajashekarappa, Dr. K M Sunjiv Soyjaudah, (2013), "Overview of Differential Cryptanalysis of Hash Functions using SMART Copyback for Data", at International Journal of Computer Science and Technology (IJCST), Vol. 4, Issue 1, pp 42-45.

[2]. Biham, E., and Shamir, A, (1993), Differential Cryptanalysis of the Data Encryption Standard. NewYork: Springer-Verlag.

[3]. Comppersmith, D, May, (1994), "The Data Encryption Standard (DES) and Its Strength Against Attacks", IBM Journal of Research and Development.

[4]. Matsui, M,(1993), "Linear Cryptanalysis Method for DES Cipher." Proceedings, EUROCRYPT '93, published by Springer-Verlag.

[5]. Rajashekarappa, Dr K M Sunjiv Soyjaudah, (2012), ICIP, Cryptanalysis of Simplified-Data Encryption Standard Using Tabu Search Method, pp. 561-568, ©Springer-Verlag Berlin Heidelberg.

[6]. William Stallings, "Cryptography and Network Security Principles and Practices", Fourth edition, McGraw- Hill, 2003.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[7]. Behrouz A. Forouzan, (2006)"Cryptography and Network Security", Firstedition, McGraw- Hill.

[8]. James Kennedy and Russell Eberhart,(1995) "Particle Swarm Optimisation", Proceedings of the IEEE International Conference on Neural Networks,pp.1942-1948.

[9]. Chanas S. and P. Kobylanski,(1996) "A New Heuristic Algorithm Solving the Linear Ordering Problem", Computational Optimization and Applications, Vol. 6, pp. 191-205.

[10]. Lan Sommerville, (2006) "Software Engineering", Sixth Edition, Pearson Education Asia.

[11]. Chanas, S., Kobylanski, P, (1996), A New Heuristic Algorithm Solving the Linear Ordering Problem. Computational Optimization and Applications 6, 191–205.

[12]. Atul Kahate, "Cryptography and Network Security", TMH, 2003.

[13]. C. Harpes, G.G. Kramer, J. L. Massey,( 1995), A Generalization of Linear Cryptanalysis and Applicability of Matsui's piling-up Lemma", Advances in Cryptology Eurocrypt'95, Sprmger Verlag, ISBN3-540-59409-4.

[14]. B. S. Kaliski Jr., M.J.B Robshaw,( 1994), Linear Cryptanalysis Using Multiple Approximations", Advances in Cryptology Crypto'94, Springer Verlag, ISBN 3-540-58333-5.

[15]. L.R. Knudsen,(1994), "Truncated and Higher Order Differentials", Second International Workshop on Fast Software Encryption, Lueven, Belgium, pp. 196–211.

[16]. A.Zugaj, K. Górski, Z. Kotulski, A. Paszkiewicz, J. Szczepański,(2000) "New constructions in linear cryptanalysis of block ciphers", ACS'2000, October.

[17]. Rajashekarappa and Dr. K M S Soyjaudah, 2012, "Heuristic Search Procedures for Cryptanalysis and Development of Enhanced Cryptographic Techniques" Published at International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.3, pp-949-954.

[18]. M. Albrecht and C. Cid, 2009, "Algebraic techniques in differential cryptanalysis", Fast Software Encryption,16th International Workshop, FSE 2009, Leuven, Belgium, February 22-25, 2009, Revised Selected Papers, Lecture Notes in Computer Science, vol. 5665, Springer, pp. 193–208.

[19]. Baudoin Collard and Francois-Xavier Standaert, 2011, Experimenting Linear Cryptanalysis. In Pascal Junod and Anne Canteaut, editors, Advanced Linear Cryptanalysis of Block and Stream Ciphers, volume 7 of Cryptology and Information Security Series. IOS Press.

[20]. Leander, G, 2010, Small scale variants of the block cipher PRESENT. Cryptology ePrint Archive, Report 2010/143 (2010) http://eprint.iacr.org/2010/143.

[21]. Jiqiang Lu, 2012, "A Methodology for Differential-Linear Cryptanalysis and Its Applications",Fast Software Encryption International Workshop, FSE2012,Singapore.

[22]. M. Hermelin, K. Nyberg, 2010, Dependent Linear Approximations: The Algorithm of Biryukov and Others Revisited, in the proceedings of CT-RSA 2010, LNCS, vol 5985, pp 318-333, San Franciscon California, USA, February 2010.

**Rajashekarappa** working as a Lecturer since July 2010 in the Department of Computer Science and Engineering, JSS Academy of Technical Educational, Avenue Droopnath Ramphul, Bonne Terre, Vacoas, Mauritius. He has one and half years of experienced as a Project Assistant at Indian Institute of Science (IISc), Bangalore, India. He worked as Project Internee in Indian Space Research Organization (ISRO), Bangalore, India. He has one and half years of experienced as a Project Trainee at LSI Technologies Pvt. Ltd, Bangalore, India. Mr. Rajashekarappa obtained his Bachelor of Engineering in Computer Science and Engineering from Anjuman Engineering College, Bhatkal, India. He has qualified in Graduate Aptitude Test in Engineering (GATE), Computer Science and Engineering, 2006. He received his Master Degree in Computer Science and Engineering from R. V. College of Engineering, Bangalore, India. He is pursuing his Ph. D in Computer Science and Engineering at Jain University, Bangalore, India. His area of interest and research include Cryptography, Data mining, Mobile Communication, Computer Networks and Cloud Computing. He has published several Research papers in international journal/conferences. He has guided many students of Bachelor degree in Computer Science and Engineering in their major projects. Mr. Rajashekarappa is a member of ISTE, IETE, IACSIT, IAEST, IAENG and AIRCC.

**K M Sunjiv Soyjaudah** received his B. Sc (Hons) degree in Physics from Queen Mary College, University of London in 1982, his M.Sc. Degree in Digital Electronics from King's College, University of London in 1991, and his Ph. D. degree in Digital Communications from University of Mauritius in 1998. He is presently Professor of Communications Engineering in the Department of Electrical and Electronic Engineering of the University of Mauritius. His current interest includes source and channel coding modulation, image processing, cryptography, voice and video through IP, as well as mobile communication. Dr. K M S Soyjaudah is a member of the IEEE, Director in the Multicarrier (Mauritius), Technical expert in the Energy Efficiency Management Office, Mauritius. Registered PhD Guide in University of Mauritius, Reduit, Mauritius, and Jain University, Bangalore, Karnataka, India.

**Sumithra Devi K A,** Professor and Director, in Master of Computer Applications at R V College of Engineering, Bangalore, India. She received B.E. from Malnad College of Engineering, Hassan. She received M.E and Ph D from UVCE, Bangalore and Avinashilingam University for Women, Coimbatore, INDIA respectively. Reviewer for many International Journals / Conferences like WEPAN, WICT, EDAS, IACSIT, ISCAS, JEMS, Published 14 journals and 65 International/ National Conferences. Professional Member in many IEEE, IETE, CSI, ISTE. Member in BoS and BoE, for Visvesvaraiah Technological University, Belgaum, Karnataka. Registered PhD Guide in Visvesvaraiah Technological University, Belgaum; Jain University, Bangalore; Prist University, Sathyabhama University, Tamilnadu. Authored a chapter "CAD algorithm for VLSI design" in the book "VLSI Design ", published by In-Tech Publications, ISBN 979-953-307-512-8, 2011, and authored book on Operating System, published by Shroff Publisher India