ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Implementation of Secure Data Transmission Scheme by Using Encryption Based Technique

Nikita D.Dongare [1], Prof. H. R. Vyawahare [2]

ME Student, Department of Computer Science & Engineering Sipna C.O.E.T Amravati, Maharashtra, India[1]

Associate Professor, Department of Computer Science & Engineering, Sipna C.O.E.T Amravati, Maharashtra, India [2]

ABSTRACT*:*Security of data transmitted through internet has put a number of challenges. Reliability issues regarding to data transmission such as confidentiality, data security and data loss are becoming serious concerns. For overcome this problem we combine two techniques that are encryption and compression, which provides a strong backbone for its security and reduces extra overhead. In this paper, we describe the encryption mechanism, which uses the pattern matching to reduce the channel overhead and also uses the compression technique. By using this method the system can reduce unwanted space and also can minimize the time required to transmission of data from source to destination. This system can maintain the security by using encryption mechanism. This scheme extends security by incorporating pattern recognition, data encryption using encryption technique, and reduces extra overhead by data compression technique.

KEYWORDS: SDES Encryption algorithm, Data compression, Deflate algorithm,

I. Introduction

Introduction is an act or process of making something known for the first time. In this propose system introduce technique for secure transmission of textual data.

In the modern digital world internet has become a predominant medium through which communication takes place. Secrecy, privacy, confidentiality are some of the primary entity that every internet user demands. Information security is a study dealing with sending and receiving the data safely and securely. Cryptography and Steganography are the two major information securing technique. Fundamentally both cryptography and steganography are information securing technique but they differ in their implementation. Cryptography makes secret data unreadable by a third party, whereas steganography hides secret data from a third party. Both of their notion remain the same. The cover medium suitable for a steganography can be any entity that can be digitally represented such as a text file, image, audio, video and TCP/IP packets. Steganography is an information hiding technique which hides the very existence of communication which takes. With respect to image and text Steganography with the advent of the Internet, computer users started to distribute, share, and transmit their private data online in a complete overt manner .In this proposed methodology system taking an input as carrier text then encrypt that carrier text using Simplified-DES algorithm and sample that carrier encrypted text and hiding our secret binary or confidential data in encrypted carrier text. Then generate the stego text and stego key after that we are compress the key and text by using lossless compression technique. Then we are extracting a secret data by taking encrypted carrier sample and stego key[1].

The S-DES encryption algorithm takes an 8-bit block of plaintext (example: 10111101) and a 10-bit key as input and produces an 8-bit block of ciphertext as output. The S-DES decryption algorithm takes an 8-bit block of ciphertext and the same 10-bit key used to produce that ciphertext as input and produces the original 8-bit block of plaintext. The encryption algorithm involves five functions: an initial permutation (IP); a complex function labeled f*K*, which involves both permutation and substitution operations and depends on a key input; a simple permutation function that switches (SW) the two halves of the data; the function f*K* again; and finally a permutation function that is the inverse of the initial permutation (IP–1).

Then we are hiding the secret text in carrier text. Four types of carrier generally used in steganography are audio, video, text and images .Hiding information in text is the most important method of Steganography. The method was to hide a secret message in every nth letter of every word of a text message. After booming of Internet and different type of digital file formats it has decreased in importance [2].The carriers may be plain text, webpage text or binary file. The

DOI: 10.15680/IJIRCCE.2016. 0405227

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

size of stego key is same as the stego text. Communication of information over the Internet is rapidly increasing due to the progression of higher availability of the Internet and the increase in bandwidth transmission speed. However, reliability issues regarding to data transmission such as confidentiality, data security and data loss are becoming serious concerns.

The process of detecting Steganography and its use is known as Steganalysis.

❖ There are two types of Steganalysis

1. Passive Steganalysis:
   Presence of hidden data is detected.

2. Active Steganalysis

Attempt is made to retrieve hidden data. Due to a number of hiding process and algorithms, detection has always been a difficult task and time consuming. So, detection is still an active area of research. The Modern Day Techniques of Steganography, Digital Hiding. There are a number of digital technologies namely movie images, audio, text files, and still images that are used for Digital Steganography.

II. RELATED WORK

S. Bhattacharjee; et al [1], the authors in this paper, presented proposed technique, which is independent of the bit stream. Hence, if some of the bits are modified or lost during the travelling time, it does not significantly impact the original data. This is the main advantage of this approach. As the compression technique reduces the output file in very small size, so the channel overhead will be significantly low. The proposed algorithm is also time efficient for both data incorporation and retrieval.

S. Das; et al [2], the author in this paper, different techniques are discussed for embedding data in text, image, audio/video signals and IP datagram as cover media. All the proposed methods have some limitations. The stego multimedia produced by mentioned methods for multimedia steganography are more or less vulnerable to attack like media formatting, compression etc. In this respect, IP datagram steganography technique is not susceptible to that type of attacks. Steganalyis is the technique to detect steganography or defeat steganography.

Alaa R. Alameldeen; et al [3], the author in this paper, Propose Cache designers might consider using cache compression to increase cache capacity and reduce off-chip bandwidth. In this document, we propose and evaluate a simple significance-based compression scheme suitable for cache lines, since it has a low compression and decompression overhead. This scheme, Frequent Pattern Compression (FPC) compresses individual cache lines on a word-by-word basis by storing common word patterns in a compressed format accompanied with an appropriate prefix. This simple scheme provides comparable compression ratios to more complex schemes that have higher cache hit latencies.

Souvik Bhattacharyya; et al [4], in this paper the authors presented a novel approach of English text steganography method which is the improved version of the CALP. Stego text is generated by mapping each two bit of the binary sequence of the secret message through small texture/pattern changes of some alphabets of the cover text in order to achieve high level of security. From figure 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.

W. Bender; et al [5], in this paper, the author describe several techniques are discussed as possible methods for embedding data in host text, image, and audio signals. While they have had some degree of success, all of the proposed methods have limitations. The goal of achieving protection of large amounts of embedded data against intentional attempts at removal may be unobtainable. Automatic detection of geometric and non geometric modifications applied to the host signal after data hiding is a key data-hiding technology. The optimum trade-offs between bit rate, robustness, and deceivability need to be defined experimentally.

P. N. Kulkarni; et al [6], in this paper the author says the Multi-band frequency compression is a speech processing technique for improving speech intelligibility under adverse listening conditions. For use in this processing, three frequency-mapping schemes, i.e. sample-to-sample mapping, mapping by superimposition of spectral samples, and segment mapping schemes were investigated. Segment-mapping scheme achieved desired compression retaining the spectral distribution of energy, and without introducing irregular variations.

C. Dhanani; et al [7], in this paper the author says because of increasing amount of security threats protection of data is required. Steganography provides security of information by hiding it in carrier. This survey paper includes the classification of steganography techniques and techniques that already been implemented to hide information in web documents. Data hidden in the web document is less suspicious in compare of other carriers because HTML WebPages are now a routine part of everyone's life and html document contains the considerable number of tags, attributes & other elements in which data can be hidden.

Dr. K. M. Sunjiv Soyjaudah; et al [8], in this paper the author has demonstrated that the tabu search and simulated annealing are ideally suited for the cryptanalysis of Simplified 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 Simulated Annealing Algorithm. Experimental results demonstrate good performance for tabu search than simulated annealing few parameters need to be tuned for the best possible performance.

Sheelu [9], propose Steganography not only prevents others from knowing the hidden information, but it also prevents others from thinking that the information even exists. If a Steganography method causes someone to suspect there is secret information in a carrier medium, then the method has failed. Different file formats can be used as carrier in Steganography

III. METHODOLOGY

Communication of information over the Internet is rapidly increasing due to the progression of higher availability of the Internet and the increase in bandwidth transmission speed. However, reliability issues regarding to data transmission such as confidentiality, data security and data loss are becoming serious concerns. The Client requires that; the transmitted data should not be lost, damaged or manipulated by any unauthorized third party. Data lost can also result from network congestion due to extra overhead. The objective of this system is to provide an integrated mechanism which can resolve security issues, provide confidentiality, and reduce information loss [10].

3.1 Cryptography

Since the ancient times and all the way till now people have been transferring secret messages. Ones only in the military and the state affairs, and by spreading of electronic communications in all areas of human activities; data protection, security and privacy are becoming issues of extremely important interest. By development of the electronic banking and commerce this topic also becomes more interesting in economy. Before we proceed to more specific analysis, we will define the basic concepts related to this work

3.1.1 Simplified-DES

This section briefly gives the overview of S-DES Algorithm. The SDES encryption algorithm takes an 8-bit block of plaintext and a 10-bit key as input and produces an 8-bit block of cipher text as output. The decryption algorithm takes an 8-bit block of cipher text and the same 10-bit key used for encryption as input and produces the original 8-bit block of plaintext as output[11]. The encryption algorithm uses five basic functions:

1. An initial permutation (IP).
2. A complex function called fK which involves both permutation and substitution operations and depends on a key input
3. A simple permutation function (SW) that switches the two halves of the data.
4. The function fK a TS in and
5. A permutation function that is the inverse of the initial permutation (IP-1). The function fK takes as input the data passing through the encryption algorithm and an 8-bit key.

DOI: 10.15680/IJIRCCE.2016. 0405227

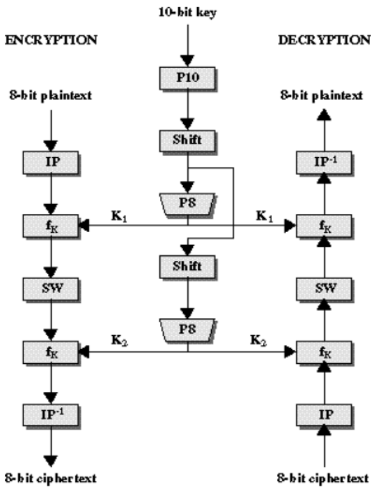

Figure 3.1.1:-SDES encryption

3.3. Data compression

Data compression is used to reduce the size of data stored in digital files. Examples of digital files are: scanned images, computer files of natural language text, computer programs, binary executable files, multimedia files etc. Now, with the wide use of internet applications, there is an increase in the data transmission over communication links. Some examples are email, chat, distributed computing, social networking, cloud computing, online videos, online conferences, data transfer from mobile to servers etc. Larger the data to be transmitted, larger is the use of communication bandwidth and communication time. Compression is a well-defined approach for reducing the number of bits needed to store or transmit data over the network [12-14].

- **Huffman Coding**:-

  Given a set of data symbols or alphabet and their frequencies occurrences, build a set of variable-length code words with the smallest average length and assign them in the place of these symbols. Here each time two symbols with the smallest probabilities are selected, and added to the top of the partial tree, deleted from the list, and replaced with an auxiliary symbol representing the two original symbols. When the list is reduced to just one auxiliary symbol, the tree is complete. The tree is then traversed to determine the code words of symbols and replaced with their corresponding code words

- **Run Length Encoding**:-

In this approach, any sequence of identical symbols will be replaced by the number of repetitions of this particular symbol followed by this particular symbol. For instance, the text 'aaaa' is coded as '4a'. RLE is widely used in early graphics file format for compressing black and white images.

- **Lempel Ziv:**

It is the dictionary-based encoding technique. Some predefined codes represent the sequence of characters from matching previously stored database. In this mechanism the search is done within the search buffer and the longest matching string is taken to replace the character or symbols.

- **DEFLATE algorithm**: -

It combines both LZ77 and Huffman compression technique to compress data. LZ77 is a dictionary-based compression technique, so it uses a 32K sliding window to record the repetitive characters. In present scenario, many software implementations such as PKZIP, zlib/gzip, 7-Zip/Advance COMP use Deflate algorithm. It searches duplicated strings in input data. Second occurrence of a string is replaced by a pointer to previous string, in form of a pair.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

IV. RESULT ANALYSIS

Name of security Scheme	Maximum Key Length	Can prevent Sniffer and Chosen Sniffer Attack
AES	32 Bytes	False
DES	8 Bytes	False
Tripple DES	24 Bytes	False
Blowfish	56 Bytes	False
RSA	128 Bytes	False
SDES	10 Bits	True (for extraction we need decrypted stego text stego key and mapping table)
Carrier sampling		

Table 4.1:-Comparison among different security technique

In this table we calculate the ratio of compression text and compare our proposed compression ratio with existing Huffman compression technique. And in this result our compression ratio is better than Huffman technique.

Text File	Huff time in (sec)	Proposed system time (sec)
27	0.1846	0.009
84	0.1771	0.011
139	0.1747	0.014
195	0.1751	0.032
320	0.1825	0.037

Table 4.2:- Compression time in second

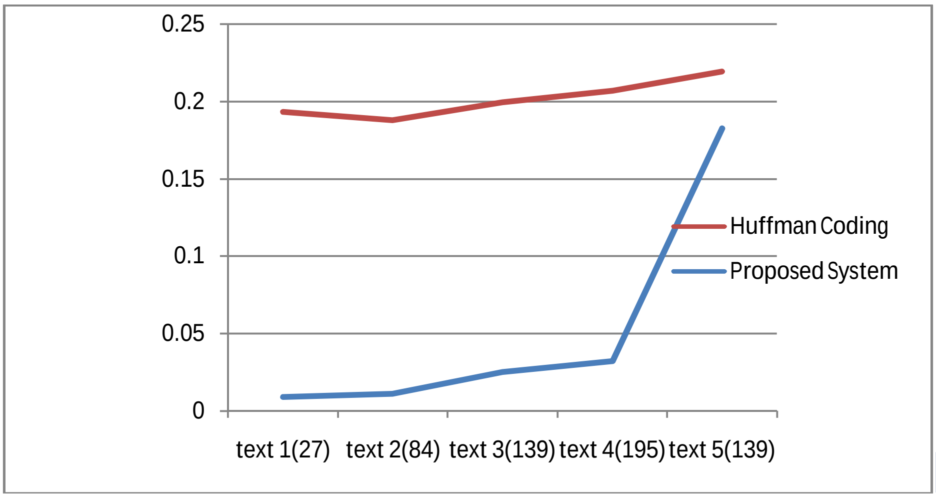

Fig.4.3 Comparative graph of Huffman Coding and Proposed System

DOI: 10.15680/IJIRCCE.2016. 0405227

Text File	Encryption Time Analysis
Text1(27)	1.383 sec
Text2(84)	1.519 sec
Text3(139)	2.458 sec
Text4(195)	1.706 sec
Text5(320)	4.288 sec

Table 4.4 Encryption time analysis

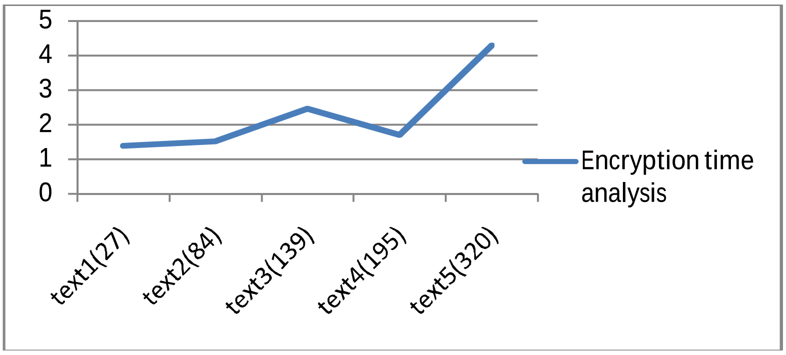

Fig.4.5 Graph of Encryption time analysis

Now we can calculated the Encryption time only and analysis the time required for execute the text, after that we can run text by combine with compression algorithm and again check for time required to run the text.

Text File	Compression Time Analysis
Text1(27)	0.009 sec
Text2(84)	0.011 sec
Text3(139)	0.014 sec
Text4(195)	0.008 sec
Text5(320)	0.062 sec

Table 4.6 Compression Time Analysis

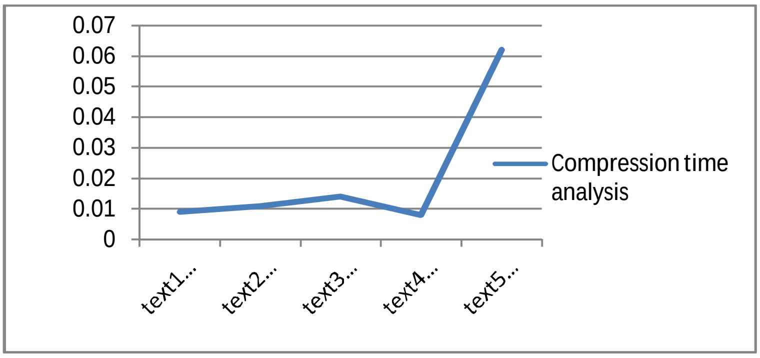

Fig.4.7 Graph for Compression time analysis

Below table shows the combine time analysis for Encryption & Compression algorithm. In this table we check the difference of time required by both graph with compression and without compression. Due to this we can make difference in both technique.

Text File	**Combine time Analysis for Encryption & Compression**
Text1(27)	1.392
Text2(84)	1.530
Text3(139)	2.472
Text4(195)	1.714
Text5(320)	4.350

Table 4.8 Combine Time for Encryption & Compression

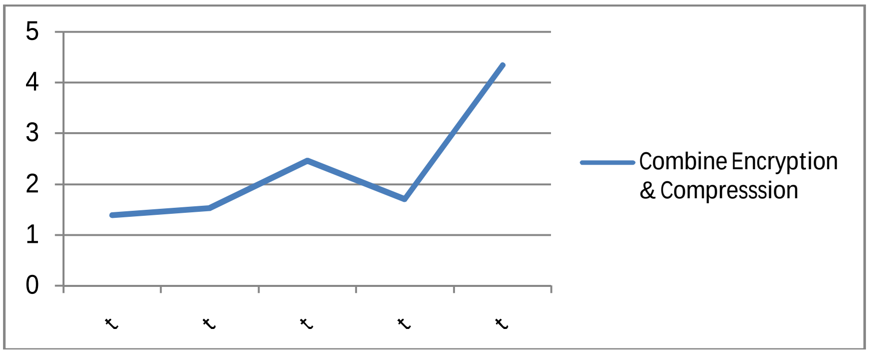

Fig.4.9 Combine graph for Encryption and Compression

We can shows that the time required by combining both algorithm that is Encryption and Compression takes less time as compared to earlier methods

Text File	**Decryption time analysis**
Text1(27)	1.017
Text2(84)	1.773
Text3(139)	1.731
Text4(195)	1.419
Text5(320)	3.847

Table 4.10 Decryption time analysis

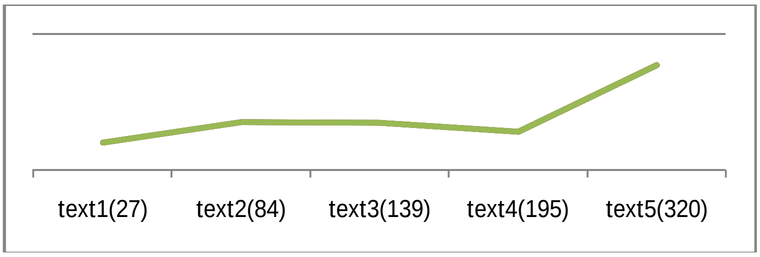

Fig 4.11 Graph for Decryption time analysis

Text File	Combine time for Decryption & Decompression
Text1(27)	1.023
Text2(84)	1.781
Text3(139)	1.746
Text4(195)	1.439
Text5(320)	3.878

Table 4.12 Combine time for Decryption & Decompression

The above graph shows the combined time for Decryption and Decompression, by using both algorithm times required for executing the text should be minimize

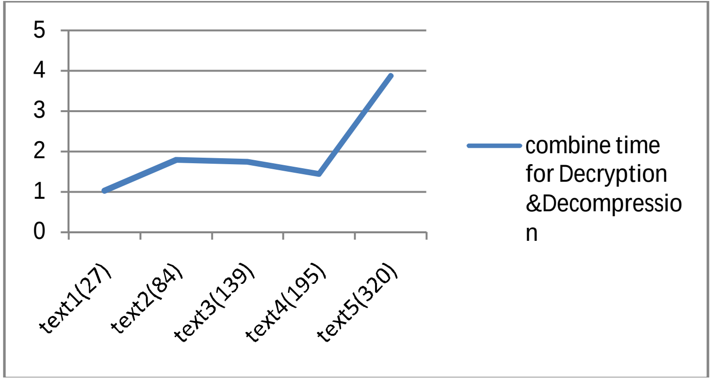

Fig.4.12 Combine graph of decryption and decompression

V. CONCLUSION

In this thesis, the propose system present the Implementation of secure data by the SDES encryption mechanism with DEFLATE compression technique .Which combine the LZ77 and Huffman compression to compress data and also reduces the time & space require to storage. In this propose system we calculate the ratio of compression text and compare our proposed compression ratio with existing Huffman compression technique. It maximizes the data security during data transmission over the network. This scheme extends security by incorporating data encryption using SDES encryption technique, and reduces extra overhead by data compression technique. The proposed algorithm is also time efficient for both data incorporation and retrieval.

REFERENCES

[1] Shiladitya Bhattacharjee1, Lukman Bin Ab. Rahim2, Izzatdin B A Aziz, “ A Secure Transmission Scheme for Textual Data with Least Overhead,” 978-1-4799-2361-8/14/$31.00 ©2014 IEEE.

[2] Roopam Bamal, Dr. V. P Singh Kaushal, “Steganography: A Modern Day Art And Science For Data Hiding,” International Journal of Latest Research in Science and Technology ISSN (Online):2278-5299Volume 2, Issue 4 :Page No.9-14, July - August (2013).

[3] Miss. Sayali S. Khadse, Prof. Dhananjay M. Dakhane, “An Immune Transposal Pattern for Text Data with Least Overhead,” International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 4, April 2015 ISSN: 2277 128X.

[4] P. N. Kulkarni and P. C. Pandey, “Frequency Mapping for Multi-band Frequency Compression for Improving Speech Intelligibility,” Proc. 14th National Conference on Communications 2008 (NCC 2008), Bombay, India.

[5] Souvik Bhattacharyya, PabakIndu2, Sanjana Dutta , Ayan Biswas4and GautamSanyal,” Text Steganography using CALP with High Embedding CapacitySouvik,” Journal of Global Research in Computer Science Volume 2, No. 5, May 2011.

[6] W. Bender,D. Gruhl, N. Morimoto, A. Lu, “Techniques for data hiding,” IBM Systems Journal, VOL 35, NOS 3&4, 1996.

[7] Chintan Dhanani, Krunal Panchal, “Steganography using web documents as a carrier: A Survey,” Steganography using web documents as a carrier: A Survey | ISSN: 2321-9939.

[8] Rajashekarappa, Dr. K M SunjivSoyjaudah, “Comparative Cryptanalysis of Simplified-Data Encryption Standard Using Tabu Search and Simulated Annealing Methods,” International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN : 2278-800X, www.ijerd.com Volume 5, Issue 3 (December 2012), PP. 07-12 7.

[9] Sheelu, “Enhancement of Data Hiding Capacity in Audio Steganography,” IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 3 (Jul. - Aug. 2013), PP 30-35.

[10] Rupali Gawade, Priyanka Shetye, Vaibhavi Bhosale, P N. Sawantdesai, “Data Hiding Using Steganography For Network Security,” International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014.

[11] Alaa R. Alameldeen and David A. Wood, “Frequent Pattern Compression: A Significance-Based Compression Scheme for L2 Caches,” Technical Report 1500, Computer Sciences Dept., UW-Madison, April 2004.

[12] Vimalathithan. R, Dr. M. L. Valarmathi, “Cryptanalysis of S-DES using Genetic Algorithm,” International Journal of Recent Trends in Engineering, Vol 2, No. 4, November 2009.