A Research on Secure Transmission of Multimedia Objects

[1] MEENAKSHI R, [2] SHWETHA T P
LECTURER
Department of Computer science and Engineering,
Government Polytechnic College Bellary, Ballari,India

***Abstract*—** Secure Transmission of different multimedia objects like image, text, audio, and video are the most demanding aspects in the internet and network application. Recently, network security is the most important issue of the internet. Cryptography is the main category of computer security that changes the information from its normal form into an unreadable form. Encryption techniques are used to securely transmit data in open networks. Steganography is used for hiding the information. This paper provides a comparative study of different methods for end to end secure transmission of multimedia objects.

Keywords- Cryptography, Encryption, Multimedia, Security.

1. INTRODUCTION

Multimedia content is a combination of image, text, audio, and video. Multimedia security deals with the methods of protecting the multimedia objects. Symmetric key algorithms are most acceptable for encrypting this multimedia objects. Here, AES algorithm is used for the encryption and decryption process of multimedia objects. Some existing symmetric key algorithms like DES, triple DES with 3 keys and AES have been implemented in different papers. Out of these algorithms AES algorithm takes minimum time to encrypt and decrypt the multimedia object with various sizes. DES and Triple DES are not considered as secure algorithms, since some attacks have been found on both algorithms. AES with 128 bit key has showed to be a secure and efficient algorithm.

1.1 Basics of Cryptography

Multimedia security is based on cryptography. In fact, some basic concepts from cryptography are used as building blocks (primitives) for applications in multimedia security. For a better understanding of issues concerning security of multimedia data, an overview of cryptography is presented at first.

1.1.1 Definition and Goals of Cryptography

Cryptography is a study of techniques (called cryptosystems) that are used to accomplish the following four goals:

- Confidentiality
- Data Integrity
- Authentication
- Non-repudation

A study of techniques used to break existing cryptosystems is called *cryptanalysis*. Since cryptography and cryptanalysis are greatly dependent of each other, people refer to *cryptology* as a joint study of cryptography and cryptanalysis.

Let us spend some time trying to understand all four goals of cryptography. *Confidentiality* means that the communication material is confidential and that it is only accessible to the desired communicating parties. An undesiredcommunicating party (called adversary) must not be able to access the communication material. This goal of cryptography is a basic one, onethat has been always addressed and enforced throughout the history of cryptographic practice. *Data integrity* means that the communication material cannot be altered in any way. If the information is altered, all communicating parties can detect this. Means of authenticating desired communicating parties is referred to as *authentication*. One of the main examples of authentication includes digital signatures. Finally, *non-repudation* means that the receiver can prove to everyone that senderdid indeed send the message; i.e., the sender cannot claim that he or she didn't encrypt and/or sign certain digital information. Fortunately, modern cryptography has developed techniques to handle all four goals of cryptography.

Today, there are two types of cryptosystems: symmetric (private) key cryptosystems and asymmetric (public) key cryptosystems. Most people have chosen to call the first group simply *symmetric key cryptosystems*, and the popular name for the the second group is just *public key cryptosystems*.

Today, there are two types of cryptosystems: symmetric (private) key cryptosystems and asymmetric (public) key cryptosystems. Most people have chosen to call the first group simply symmetric key cryptosystems, and the popular name for the the second group is just public key cryptosystems.

1.2 Symmetric Key Cryptosystems

Symmetric key cryptosystems have been around for thousands of years. All classical cryptosystems (that is cryptosystems that were developed before 1970s) are examples of symmetric key cryptosystems. In addition, most modern cryptosystems are symmetric as well. Some of the most popular examples of modern symmetric key cryptosystems include AES (Advanced Encryption Standard), DES (Data Encryption Standard), IDEA, FEAL, RC5, and hundreds of others.

All symmetric key cryptosystems have a common property: they rely on a shared secret between communicating parties. This secret is used both as an encryption key and as a decryption key (thus the keyword "symmetric" inthe name). This type of cryptography ensures only confidentiality and failsto provide the other three goals of cryptography. Even more importantly,the disadvantage of symmetric key cryptography is that it cannot handle large communication networks. If a node in a communication network of n nodes needs to communicate confidentially with all other nodes in the network, it needs n 1 shared secrets. For large n this is highly impractical and inconvenient. On the other hand, the big advantage over public key cryptosystems is that symmetric cryptosystems require much smaller key sizes for same level of security. Therefore, computations are much faster, the memory requirements are much smaller, and much smaller computational power is sufficient.

1.3 Public Key Cryptosystems

In public key cryptography there are two different keys, one called a *public key* is the key that should be publicly known, while the so-called *secret key* should be kept secret by the owner. The birth of the public key cryptographyis credited to Whitfield Diffie and Martin Hellman. The powerful idea that they introduced was to use a mathematically intractable and computationally infeasible problem(s) as a security basis. The system is asymmetric since there are two different keys used: public key and private key. If data is encrypted with public key, it can only be decrypted using the correspondingprivate key, and vice versa. Today, all public key cryptosystems rely on some intractable problem. For example, cryptosystem RSA relies on difficulty of factoring large integers, while El-Gammal cryptosystem relies on the discrete logarithm problem (DLP) which is the problem of finding a logarithm of a group element with generator base in finite abelian group. Originally proposed Diffie-Hellman protocol relies

on DLP as well. The beauty is that all public key cryptosystems do not need to have a shared secret between communicating parties. This solves the problem of large confidential communication network introduced earlier. In addition, public key cryptography opened door for ways of implementing technologies to ensure all four goals of cryptography. By means of combining the public key cryptography, public key certification, and secure hash functions, there are protocols that enable digital signatures, authentication, data integrity and non-repudation. Unfortunately, due to processor speed growth and even more due to smart modern cryptanalysis, the key sizes for public key cryptographygrew very large. This gave a disadvantage in comparison to symmetric key cryptosystems: public key cryptography is significantly slower, requires large memory capacity, and large computational power. Just for comparison 128bit key used with DES cryptosystem has approximately the same level of securityas the 1024bit key used with RSA cryptosystem [AMV97]. To solve these problems, researchers introduced different approaches. In order to decrease key sizes so the public key cryptography can be used in smaller computational environments (such as smart cards or handheld wireless devices), Neil Koblitz introduced the idea of using more exotic group in the public key underlying algebraic structure: the elliptic curve group. Elliptic curve cryptography (much of whose implementation is credited to CertiCom) enables smaller key sizes of public key cryptosystems that rely on DLP. The elliptic curve group algebra is much more complex so the cryptanalysis is much harder, resulting in smaller key requirements. Another solution came from public key cryptosystems that initially use more complex computational problem, suchas lattice reduction problem. Relatively new cryptosystem NTRU [JH98], based on the algebra of a ring of truncated polynomials, relies on lattice reduction problem and it is the only public key cryptosystems that have the speed, memory, and computational complexity comparable to symmetric key cryptosystems. However, since this system is relatively new, the underlying security of NTRU is yet to be investigated.

There is more popular approach in resolving the complexity of public key cryptosystems and that is combining the existing symmetric key cryptography with existing public key cryptography. This hybrid approach is very much widely accepted since it enables the optimal choices of the hybridcomponents. A fast symmetric key cryptography can be used in most of thelengthy communication, but the required shared secret can be shared on thefly using some public key scheme. Furthermore, the same public key scheme can be used to accomplish other three goals of cryptography. The most important is to enable speedy performance on the lengthy communication material. Using public key cryptography only to transmit the symmetric key or to authenticate digital signature will not significantly affect the performance.

2 COMMUNICATION CRYPTOGRAPHY VS. DIGITAL RIGHTS MANAGEMENT

that wants to access the communication information by listening to the communication channel. This model assumes that the channel end-points are trusted.

In contrast, DRM cryptography deals with a scenario in which unicasting, multicasting, or broadcasting party needs to securely transmit the content to the pool of trusted devices. In this model, an adversary is not only the channel eavesdropper. The users of the trusted device can also potentially be adversaries. A user of the trusted device can view the content but should notbe able to distribute the content. Eavesdropper shouldn't be able to neitherview nor distribute the valuable content.

3 MULTIMEDIA CONTENT CRYPTOGRAPHY

In this section, we present the relevant topics regarding cryptography in respect to multimedia data. In this section, we present the relevant topics regarding cryptography in respect to multimedia data.

a. Multimedia and Multimedia Security

Multimedia is a combination of the following media: text, still images, audio data, animation, and video. Multimedia security in general is a method or a set of methods used to protect the multimedia content. These methods are heavily based on cryptography and they enable either communication security, or security against piracy (DRM security), or both.

Communication security of digital images and textual digital media can be accomplished by means of standard symmetric key cryptography. Such media can be treated as binary sequence and the whole data can be encrypted using cryptosystem such as AES or DES [Sti02]. In general, when the multimedia data is static (not a real-time streaming) we can treat it as a regular binary data and use the conventional encryption techniques. Encrypting the entire multimedia stream using standard encryption methods is referred to as the naive algorithm.

However, due to variety of constraints (such as near real-time speed), communication security for streaming audio and video media is harder to accomplish. Communication encryption of video and audio multimedia content is not simply the application of established encryption algorithms, such as DES or AES, to its binary sequence . It involves careful analysis to determine and identify the optimal encryption method when dealing with audio and video media. Current research is focused on modifying and optimizing the existing cryptosystems for real-time audio/video. Itis also oriented towards exploiting the format specific properties of many standard video and audio formats, in order to save desired speed and enablereal-time streaming. This is referred to as *selective encryption* [JWJ01]. Selective encryption is particularly applicable to digital cable videos. For textual media and some low-quality audio and video streaming multimedia we can still apply real-time packet encryption by means of SRTP (Secure Real-time Transport Protocol), which is based on AES and encrypts entire multimedia bitstream.

b. Identifying Encryption Level in Multimedia Communication Security

There are many different occasions where multimedia communication security is desired. However, deciding upon what level of security is neededis harder than it looks. To identify an optimal security level, we have to carefully compare the cost of the multimedia information to be protected and the cost of the protection itself. If the multimedia to be protected is not that valuable in the first place, it is sufficient to choose relatively light level of encryption. On the other hand, if the multimedia content is highly valuable or represents a government or military secrets, the cryptographic security level must be the highest possible.

For many real-world applications such as pay-per-view, the content data rateshould be very high, but the monetary value of the content may not be highat all. Thus, very expensive attacks are not attractive to adversaries, and light encryption may be sufficient for distributing such MPEG videos. For these applications, DRM is of much more interest.

On the other hand, applications such as videoconferencing or videophone (or even Internet phone) may require much higher level of confidentiality. If thevideoconference is discussing important industrial, governmental or military secrets, the cryptographic strength must be substantial. Maintaining such high level of security and still keeping a real-time and limited-bandwidth
constraints is not easy to accomplish.

4. OVERVIEW OF MAIN MULTIMEDIA FORMATS: JPEG AND MPEG

To really understand the modern approaches to the multimedia security, it is necessary to understand the structure of the JPEG and MPEG formats. Due to the popularity, most of the proposed schemes are aimed to JPEG and MPEG formats, however, some basic ideas can be naturally extended to other formats since there are similarities between them. For example similar techniques and algorithms for MPEG format can be extended to H.26x family.

a) JPEG

JPEG (Joint Photographic Expert Group) format is standardized in 1992. This is a lossy type of compression algorithm whose quality and compressionratio are inversely proportional (tradeoff). The figure below shows the stagesof JPEG encoding and decoding:

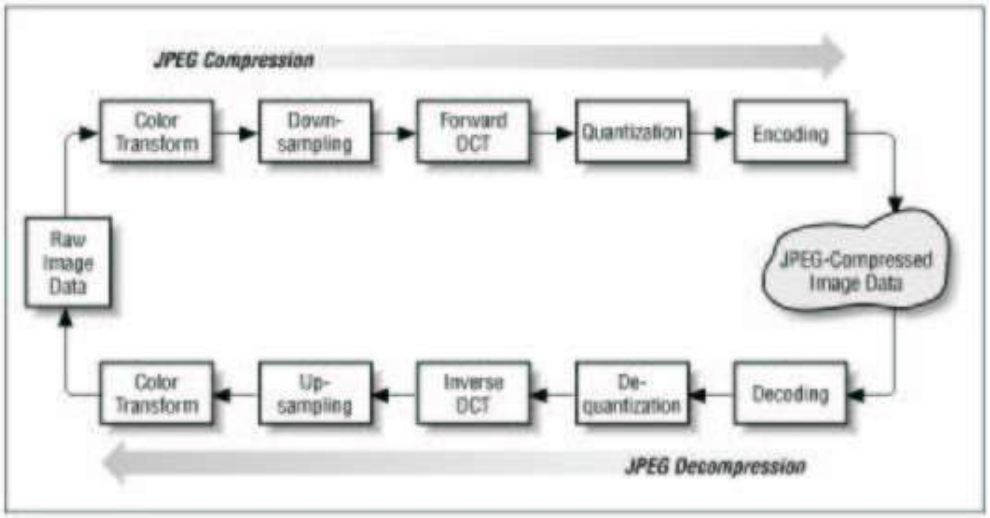

Figure 1: stages in the JPEG compression algorithm

In short, the image is divides into 8x8 blocks which undergo several stages, such as DCT (Discrete Cosine Transform), quantization (lossy stage), zig-zag sequencing, and entropy encoding based on Huffman compression. The DCTtransformed 8x8 block has the property that most information carrying bytesare the ones located at the top left corner of the block. JPEG images are building blocks for MPEG videos, which are discussed next.

b) MPEG

The MPEG acronym stands for Moving Picture Experts Group and it isthe name of the one of the most important and most widely used video codecs. The MPEG1-2 video encoding scheme represents the video signal using the repetition of group of pictures (GOPs). Each GOP is a sequence of selected I, P and B frames. Examples of GOP sequences are (IBBBPBBB) or (IBBPBBPBB), but the relative frequency of I, P and G frames maybe application dependent. I frames are encoded as standard JPEG images, without reference to other frames. Consequently, I frames are of the smallest compression ratio. On the other hand, P frames are encoded with reference to the I frames, containing only the differences between the two consecutiveframes. Since the time difference between two consecutive frames is a fraction of a second, the Humming distance between pixel blocks is very small. Therefore, P frames have much better average compression ratio than the I frames. Finally, B frames are bidirectionally interpolated using the previous closest I/P frame and the following closest I/P frame. The average compression ratio of B frames is usually the highest.

5. SECURE TRANSMISSION METHODS

Euijin Choo et al. proposed a light weight encryption scheme for secure real time multimedia transmission. That is SRMT (Secure Real-time Multimedia Transmission). SRMT is an encryption scheme without loss of security and media QoS. It provides the confidentiality of multimedia data. Here uses one XOR operation and two block transpositions. In order to provide both security and media QoS, here consider three important characteristics. That is processing time, compression rate and security level. The SRMT scheme uses two block 0 transpositions and one XOR operation. Here first transposition is for generating a key frame. Second transposition and XOR operation is main encryption process. SRMT provide faster encryption of MPEG compressed data. Here attack models are classified in to two categories. That is cipher text only attack and chosen plaintext attack.

B.Padmasri et al. proposed Spread Spectrum Image Steganography with Advanced Encryption key implementation (SSISAE). Nowadays the information hiding methods have become an important research area.This paper, explains a framework of effective security for data communication by implementing SSISAE. This system hides and recovers message. The hidden message can be retrieved using appropriate keys without any knowledge of actual image. This paper describes the spread spectrum communication that is the process of spreading the bandwidth of a narrow band signal across a wide band of frequencies. Here AES algorithm is usedfor encryption and decryption process.

A. Jaishree Singh et al. proposed secure data transmission using encrypted secret message. In this paper the secret message is encrypted before the actual embedding process starts. Here, the hidden message is encrypted using the private key. And also DCT (Discrete Cosine Transform) technique is used for embedding and extraction of files. That is this proposed system encrypts the data with a tiny algorithm and then embed this encrypted data in a cover file. For this DCT algorithm is used. This proposed system provides the security of data. Here the mini algorithm is a Feistel type cipher that uses operations from mixed algebraic groups XOR, ADD and SHIFT. This paper provides two types of security levels, first by encryption and second is embedding or steganography. The below figure depict this proposed system.

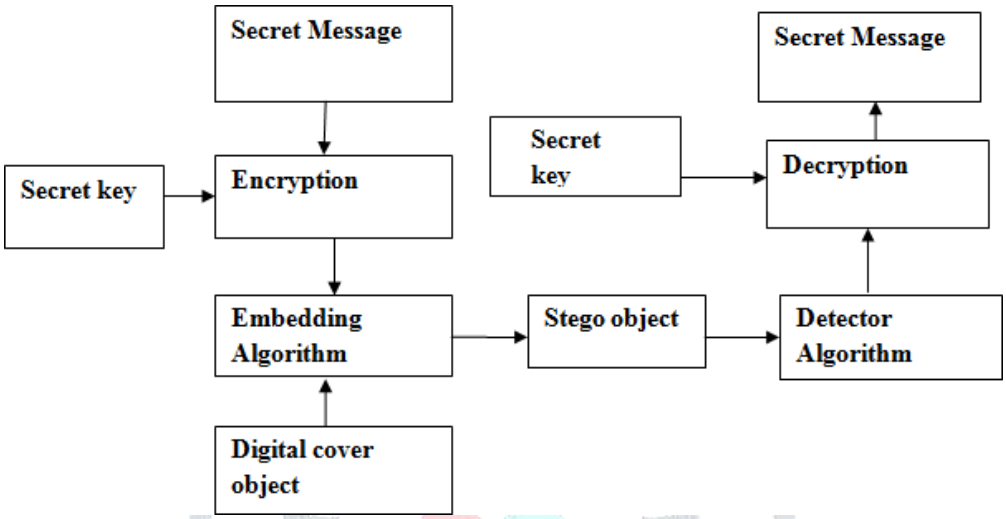

Figure 2. Block diagram of secure data transmission using encrypted messages

Parameshachari B. D. et al. proposed secure transmission of an image using partial encryption algorithm. This paper proposes a novel concept of combined partial image encryption using phase manipulation and sign encryption. The encryption process contains two stages where image to be encrypted are applied to phase manipulation block. In first stage Fourier Transform (FT) is applied to get phase and magnitude of the input image. Phase of the image are crawled to get modified image after applying Inverse Fourier Transform. In second stage the modified image is partially encrypted by using sign encryption. Sign Encryption finally gives resultant partially encrypted image by extracting the sign bits of modified image. Partial encryption is one of the most promising solutions to reduce the cost of data protection in wireless and mobile network. This paper presents a novel concept of pixel value manipulation using phase manipulation in frequency domain and sign encryption for partial encryption method.

Nagesh Sharma et al. proposed a novel technique for secure information transmission in videos using salt cryptography. This paper presents a novel technique for transmitting secret information securely from sender to receiver by embedding this information into a video after encryption through salt cryptography. In this encryption method some random data is added to the private keys and passwords. Here define this random data as a salt which is needed to access the encrypted data, along with the password. These passwords alone have no use since they will be able to locate the hidden data only when mixed with proper salt. This salt is handled by a certified third party. Salt is created for different pairs of communicating parties. Here also introduced the concept of Enterprise Dependent Value (EDD), which are the embedding values corresponding to the binary digits and are specific to the communicating enterprises.

A secure audio steganography approach presented in by Mazdak Zamani et al. This paper describes a wide range of steganography techniques. This approach resolves several problems like weakness of substitution technique and the large strength of substitution technique. An intelligent algorithm will try to embedthe message bits in the deeper layers of samples and alter other bits to decrease the error and if alteration is not possible for any samples it will ignore them. Using this proposed genetic algorithm, message bits are fixed into multiple, vague and higher LSB layers, resulting in increased robustness.

Three new selective encryption techniques for secure transmission of MPEG-I video bit streams are presented in by Adnan M. Alattar et al. These techniques improve the security level, and provide reasonable processing time. Here,

in the first method the encryption is applied to the data associated with every n^{th} I macro block. In the second method, the encryption technique is applied to the headers of the entire predicted macro block as well as to the associated with every n^{th} I macro block. In the third method, encryption is applied to every n^{th} I macro block as well as the header of every nth predicted macro block. Finally with n=2, is found to be the most efficient of the three proposed methods. This method reduces the processing time, and the simulation results show that the encrypted video is fully disguised.

Rucha Bahirat et al. is a survey on different secure data transmission using steganography. The ultimate aim of this steganography is to communicate securely in a completely invisible manner, so that no one can identify the transmission of a hidden data. This paper discusses the concept behind the steganography by describing what is steganography and the terms that are related to steganography. This paper gives the different steganography methods for image steganography, audio steganography, video steganography, and text steganography that are used to embed the information in digital media. The two most important aspects of this steganography system are the quality of stego object and the capacity of the cover media. This paper found, a better steganography approach to increase the PSNR value and to decrease the MSE. The basic form for steganography is shown in figure below. The basic model of steganography consists of cover object, message, embedding algorithm and Stego key. Nowadays steganographic systems uses multimedia objects like video, image, audio etc. as cover object because people often send out digital pictures over email and other Internet communication.

In text Steganography the secrete message is hidden in the text and we use the different method to hide the message in text by changing the last bit of the message. Taking the cover object as image in steganographyis known as image steganography. Generally, in this technique pixel intensities are used to hide the information.

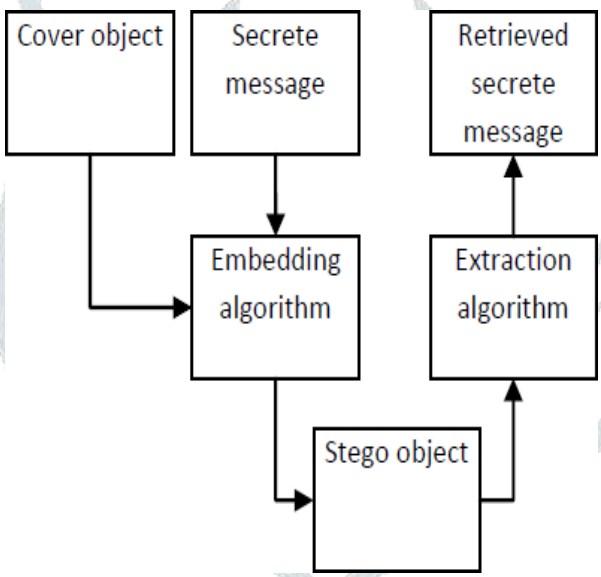

Figure 3 . Basic steganography model

In Audio steganography, secret messages are embedding in digital sound. The secret data is embedded by slightly varying the binary sequence of a sound folder. Audio Steganography software can implant messages in WAV, MIDI and even MP3 sound files. Video files are generally a group of images and sounds, so most of theexisting techniques on images and audio can be applied to video files too.

6. CONCLUSION

Security is the most challenging aspects of the internet and network application. Several authors proposed different techniques for secure transmission of multimedia elements like text, image, audio, and video. Here a survey is conducted in different methods for secure transmission if multimedia elements. Here explains two important security methods. That is cryptography and steganography. Encryption and Embedding provide higher security. Several encryption and embedding techniques explained here.

REFERENCES

[1] Euijin Choo, Jehyun Lee, Heejo Lee, Giwon Nam, "SRMT: A Lightweight Encryption Scheme for Secure Real-time Multimedia Transmission", Basic Research Program of the Korea Science & Engineering Foundation.

[2] B.Padmasri, M.Amutha surabi, "Spread Spectrum Image Steganography with Advanced Encryption Key Implementation", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013.

[3] A. Jaishree Singh, Dr. J.S. Sodhi, "Secure Data Transmission using Encrypted Secret Message", International Journal of Computer Science and Information Technologies, Vol. 4 (3) , 2013, 522-525.

[4] Parameshachari B D, K M Sunjiv Soyjaudah, Sumitrha Devi K A, "Secure Transmission of an Image using Partial Encryption based Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 63– No.16, February 2013.

[5] Nagesh Sharma, Dr. Rakesh Rathi , Vinesh Jain, Mohd. Waseem Saifi,"A Novel Technique for Secure Information Transmission in Videos Using Salt Cryptography," Information and Knowledge Management ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol.3, No.10, 2013.

[6] Mazdak Zamani, Azizah Bt Abdul Manaf, Rabiah Bt Ahmad, Farhang Jaryani, Hamed Taherdoost, Akram M. Zeki, "A Secure Audio Steganography Approach," International Islamic University Malaysia.

[7] Adnan M. Alattar, Ghassan I, AI. Regib, "Improved Selective Encryption Techniques for Secure Transmission of MPEG Video Bit- streams", IEEE, 1990.

[8] Rucha Bahirat , Amit Kolhe, "Overview of Secure Data Transmission using Steganography", International Journal of Emerging Technology and Advanced Engineering Website, Volume 4, Issue 3, March 2014.