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. 3, Issue 5, May 2015

Secured Image Recovery and Data Extraction Using Reversible Data Hiding

Usama Abdur Rahman[1], C. Anuradha*[2]

[1]Professor & Head, Dept. of CSE, Jerusalem College of Engineering, Chennai, Tamil Nadu, India

[2]Associate Professor, Dept. of CSE, Bharath University, Chennai, Tamil Nadu, India

*Corresponding Author

ABSTRACT: The project involves the technique called reversible data hiding in an encrypted image. Reversible data hiding is the technique to embed an additional message into some cover media. The original cover could be perfectly restored after extraction of the hidden message. This work adopts the technique by embedding a data into an encrypted image. To carry out this work in a simpler manner we divided the work into modules called Image Encryption, Data Embedding and Data extraction and Image recovery. The image given is first encrypted by a random sequence generated using a encryption key and XOR is performed with the pixels on the given image. After encryption, the data is embedded by partitioning the encrypted image into two blocks. The pixels are de-correlated in the flipped blocks. The original blocks often exhibit smoother than those of flipped blocks. Since border pixels are highly correlated, we adopt the side match technique to concatenate borders of the unrecovered block to the recovered block and smoothness calculation is done for the concatenated blocks to extract the data and the original image. The error rate is found to be 0.34% and the proposed work aids better method than the earlier methods for smoothness calculation in blocks and data extraction.

KEYWORDS: Image Encryption; Reversible Data Hiding.

1. INTRODUCTION

The project revolves round the concept of hiding data in an encrypted image for expeditious security. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Reversible data hiding in images is a technique that embeds data in digital images by altering the pixel values for secret communication, and the embedded image can be recovered to its original state after the extraction of the secret data. The former carries out a set of operations for the process to complete. The original work partitions an encrypted image into blocks, and each block carries one bit by flipping three LSBs of a set of pre-defined pixels. The data extraction and image recovery can be achieved by examining the block smoothness.

These two issues could reduce the correctness of data extraction. This letter adopts a better scheme for measuring the smoothness of blocks, and uses the side-match scheme to further decrease the error rate of extracted-bits. It carries out encryption using a set of encryption keys and perform a exclusive-OR with the random sequence generated, it then embeds the data been provided into the encrypted image by dividing them as blocks. The operation of data extraction is performed by smoothness function.

Finally image is retrieved by performing a side match to concatenate the recovered blocks to unrecovered blocks. The methods and techniques adopted above bring out higher efficiency in security and a lower error rate.

A. Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same.

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. 3, Issue 5, May 2015

Encryption was used to ensure secrecy in communications, such as those of spies, military leaders, and diplomats. The art of protecting information by transforming it into an unreadable format, called cipher text. Only those who possess a secret *key* can decipher the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable. In recent decades, the field has expanded beyond confidentiality concerns to include techniques for message integrity checking, sender or receiver identity authentication, digital signatures, interactive proofs and secure computation, among others.

Cryptography is a well known and widely used technique that manipulate information in order to cipher or hide their existence respectively. Cryptography scrambles a message so it cannot be understood; Even though the method provides security, a study is made to combine both cryptography and Steganography methods into one system for better confidentiality and security. Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and the receiver have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. In Cryptography, a cipher message for instance, might arouse suspicion on the part of the recipient while an invisible message created with steganographic methods will not. In fact, steganography can be useful when the use of cryptography is forbidden: where cryptography and strong encryption are outlawed, steganography can circumvent such policies to pass message covertly.

B. *Steganography*

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. In image steganography the information is hidden exclusively in images.The idea and practice of hiding information has a long history. In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave’s scalp. When the slave’s hair grew back the slave was dispatched with the hidden message . In the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size until it was the size of a typed period. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

II. SYSTEM ANALYSIS

System analysis is the study of sets of interacting entities, including computer systems analysis. It is also "an explicit formal inquiry carried out to help someone (referred to as the decision maker) identify a better course of action and make a better decision than he might otherwise have made.

A. Problem Description

The pixels in the blocks are not completely involved in the smoothness calculation. In the existing system smoothness calculation is carried out by avoiding the pixels in the borders[1]. So in the proposed system the pixels in the borders are considered for calculating the smoothness function. The correlation between blocks is ignored in the data extraction. In the existing system the data extraction is performed using smoothness calculation. But the correlation between blocks is ignored[2]. Because border pixels are highly correlated in the proposed system we adopt the side match technique to concatenate the borders of the recovered blocks to the unrecovered blocks and perform the smoothness calculation.

B. Existing System

The existing system block diagram explains the process that takes place in the system clearly. Here we have the content owner, Data hider and the receiver. The existing system contains an encryption key and a data hiding key. The existing system below does not explain the overall architecture of the system. It just explains in a block diagram in an overview [3].

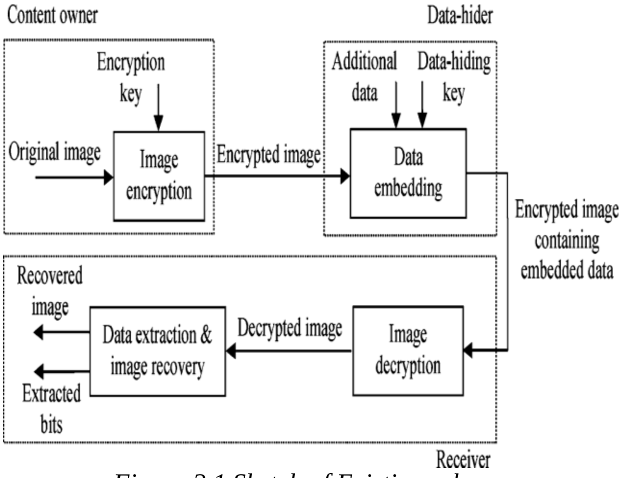

Figure 2.1 Sketch of Existing scheme

C. Proposed System

The cover image is encrypted by applying bitwise exclusive-or XOR) operator to every bit of pixels and random sequence. It is generated using an encryption key, the encryption key is converted to its binary equivalent and a circular shift is performed on that binary representation to get the random sequence[4][5]. Considering that circularly shifted sequence we have to look for the LSB's to find whether it is 0 or 1.If the sequence contains 0 at the least end, we need to take up that sequence as the random sequence else if it contains 1,now a new method is followed. Exclusive-OR is done with first obtained binary representation of that particular encryption key to obtain the so called random sequence. Then the cover image is encrypted by applying bitwise exclusive-or (XOR) operation with random sequence generated to every bit of pixels in the image as considering them as blocks of preferable block size.Atlast, convert back to its decimal form to represent the encrypted image[6]-[8].

Data embedding means embedment of the provided data into an encrypted image. According to the data hiding key pixels in each block are classified into sets s_0 and s_1 . If the data bit 0 is to be embedded then flip 3LSB's of pixels in s_0. Otherwise flip the 3LSB's of pixels in s_1

III. SYSTEM DESIGN SPECIFICATION

Systems design is simply the design of systems. It implies a systematic and rigorous approach to design—an approach demanded by the scale and complexity of many systems problems. Systems design first appeared shortly before World War II as engineers grappled with complex communications and control problems[9]. They formalized their work in the new disciplines of information theory, operations research, and cybernetics. In the 1960s, members of the design methods movement (especially Horst Rittel and others at Ulm and Berkeley) transferred this knowledge to the design world. Systems design continues to flourish at schools interested in design planning and within the world of computer science. They are also useful in modelling the design process itself.

A systems approach to design is entirely compatible with a user-cantered approach. Indeed, the core of both approaches understands user goals. A systems approach looks at users in relation to a context and in terms of their interaction with devices, with each other, and with themselves. A systems approach to design is most appropriate for projects involving large systems or systems of systems. Such projects typically involve many people, from many disciplines, working together over an extended period of time[10].

A. Introduction To Architectural Diagram

Architectural drawings are the backbone for the designers, developers and the architects. It is basic and the first element for the construction industry and for facilities management. It is always a challenge for the architects to manage their drawings as a fortune because most of them are on paper. Systems Architecture is a generic discipline to handle objects (existing or to be created) called "systems", in a way that supports reasoning about the structural properties of these objects. Systems Architecture is a response to the conceptual and practical difficulties of the description and the design of complex systems. Systems Architecture can in fact refer to:

1) The architecture of a system, i.e. a model to describe/analyze a system
2) Architecting a system, i.e. a method to build the architecture of a system
3) A body of knowledge for "architecting" systems while meeting business needs.

Systems Architecture will often rely on a tool called an architecture framework, i.e. a reference model to organize the various elements of the architecture of a system into complementary and consistent predefined views allowing covering all the scope of Systems Architecture. Famous architecture frameworks are for example DoDAF, MoDAF or AGATE.

B. *System Architecture*

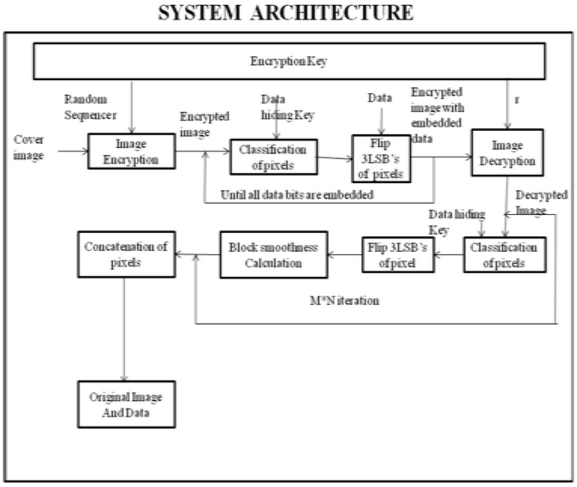

Figure.3.1 Architecture of proposed work

C. *Modules Description:*

A module description provides detailed information about the module and its supported components, which is accessible in different manners. The included description is available by reading directly, by generating a short html-description, or by making an environment check for supported components to check if all needed types and services are available in the environment where they will be used. This environment check could take place during registration/installation or during a separate consistency check for a component.

1. Image Encryption

To encrypt the cover image, we need a random sequence r .It is generated using an encryption key, the encryption key is converted to its binary equivalent and a circular shift is performed on that binary representation to get the random sequence. Considering that circularly shifted sequence we have to look for the LSB's to find whether it is 0 or 1.If the sequence contains o at the least end,we need to take up that sequence as the random sequence else if it contains 1,now a new method is followed. Exclusive-OR is done with first obtained binary representation of that particular encryption key to obtain the so called random sequence. Then the cover image is encrypted by applying bitwise exclusive-or (XOR) operation with random sequence generated to every bit of pixels in the image as considering them as blocks of preferable block size. At last, convert back to its decimal form to represent the encrypted image.

2. Data Embedding

Data embedding means embedment of the provided data into an encrypted image. To embed data, partition the encrypted image into non-overlapping blocks. According to a data-hiding key, randomly and evenly classifies pixels in each block into sets s_0 and s_1.If the bit to be embedded in this block is “0”, flip 3LSB’s of pixels in set s_0.On the contrary, if the bit to be embedded is “1,” flip 3 LSBs of pixels in Set S_1.

3. Data Extraction and Image Recovery

The encrypted image with embedded data is decrypted by performing exclusive-or (XOR) to every bit of pixels using an encryption key. According to a data-hiding key, pixels in each block are classified into sets s_0 and s_1.The block is formed by flipping 3LSB’s of pixels in set s_0.Let this block be $h^{\sim}$. Let another block be $h^{\wedge}$ which is formed by flipping 3LSB’s of pixels in set s_1.The smoothness of blocks are found for $h^{\sim}$ and $h^{\wedge}$. The difference of smoothness of blocks is sorted in descending order to extract the data and blocks. If the difference of smoothness is less than 0, then a bit 0 is extracted and $h^{\sim}$ is the original block. On contrary, a bit 1 is extracted and $h^{\wedge}$ is the original block.

D. Detailed Design

A major task of detailed design is to spell out, in detail, the attributes and methods needed by each module. Detailed design of the system is the last design activity before implementation begins. The hardest design problems must be addressed by the detailed design or the design is not complete. The detailed design should represent the system design in a variety of views where each view uses a different modelling technique. By using a variety of views, different parts of the system can be made clearer by different views. Some views are better at elaborating systems states whereas other views are better at showing how data flows within the system. Other views are better at showing how different system entities relate to each through class taxonomies for systems that are designed using an object-oriented approach. A template for detailed design would not be of much use since each detailed design is likely to be unique and quite different from other designs. What is helpful in regards to guidance on detailed design are examples.

1. Random Sequence Generation

To encrypt the cover image, we need a random sequence r .It is generated using an encryption key, the encryption key is converted to its binary equivalent and a circular shift is performed on that binary representation to get the random sequence. Considering that circularly shifted sequence we have to look for the LSB’s to find whether it is 0 or 1.If the sequence contains o at the least end, we need to take up that sequence as the random sequence else if it contains 1,now a new method is followed. Exclusive-OR is done with first obtained binary representation of that particular encryption key to obtain the so called random sequence[11].

2. Smoothness Function

The smoothness of an image block can be evaluated by calculating the absolute difference of neighbouring pixels. The larger the summation of absolute differences, the more complex the image blocks is. Therefore, we estimate the block smoothness by calculating the summation of the vertical absolute differences and horizontal absolute differences of pixels in image blocks using the following equation:

$$\sum_{u=1}^{s2}\sum_{v=1}^{s1-1}\left|p_{u,v}-p_{u,v+1}\right|+\sum_{u=1}^{s2-1}\sum_{v=1}^{s1}\left|p_{u,v}-p_{u+1,v}\right|$$

Where $p_{u,v}$ represents the pixel values located at position (u, v) of a given image block of size s1 x s2.

The Equation fully exploits the absolute difference between two consecutive pixels in both vertical and horizontal directions and thus, the smoothness of blocks can be better estimated.

3. Side Match

Since border pixels are highly correlated and the neighboring blocks are unrecovered, we adopt the side match technique to concatenate borders of the unrecovered block to the recovered block and smoothness calculation of the concatenated blocks are found to extract the data and the original block. If the recovered block is on the left or right side of the unrecovered block, then vertical concatenation of unrecovered and recovered block is made. But if the recovered block is on the top or bottom side of the unrecovered block, then horizontal concatenation of unrecovered and recovered block is made. The smoothness function is evaluated on the concatenated blocks to extract the data bit and the original block[12].

IV. IMPLEMENTATION AND RESULT ANALYSIS

Implementation is the realization of an application, or execution of a plan, idea, model, design, specification, standard, algorithm, or policy that previously exists. In computer science, an implementation is a realization of a technical specification or algorithm as a program, software component, or other computer system through computer programming and deployment. Many implementations may exist for a given specification or standard. For example, web browsers contain implementations of World Wide Web Consortium-recommended specifications, and software development tools contain implementations of programming languages. System implementation generally benefits from high levels of user involvement and management support. User participation in the design and operation of information systems has several positive results. First, if users are heavily involved in systems design, they move opportunities to mould the system according to their priorities and business requirements, and more opportunities to control the outcome. Second, they are more likely to react positively to the change process. Incorporating user knowledge and expertise leads to better solutions. The relationship between users and information systems specialists has traditionally been a problem area for information systems implementation efforts.

A. Performance Measure

Performance measurement is the process of collecting, analyzing and/or reporting information regarding the performance of an individual, group, organization, system or component. It can involve studying processes/strategies within organizations, or studying engineering processes/parameters/phenomena, to see whether output are in line with what was intended or should have been achieved. Performance measurement is carried out in the design, building, operation and maintenance of systems, machines, devices, structures, materials and processes. In design, performance measurement can be of physical properties, parameters, etc., while in maintenance, repair, and operations, and reliability, engineering, failures, downtime, uptime, maintainability and OEE are common measures[13].

Performance measurement estimates the parameters under which programs, investments, and acquisitions are reaching the targeted results. However, a model for performance set faulty may depict a disadvantageous situation which does not support the organization or the thriving to the set aims.

In spite of knowing the performance measures, it is mandatory for any system to calculate the performance measure to prove the efficiency carried out in the system. The following table explains brief about the performance measure in our project[14][15].

IMAGE	ERROR RATE OF EXISTING METHOD (%)	ERROR RATE OF PROPOSED METHOD (%)
Leena	1.21	0.34
Baboon	16.51	10
Splash	1.5	0

Table 4.1 Comparison of Existing and Proposed Method

Comparing the existing and proposed method , the proposed method recovers the image blocks more accurately than the existing method. The error rate depends on the complexity of the image. The error rate is evaluated by calculating the sum of the incorrectly recovered blocks and the the percentage of it is found. For the complex image like baboon , the error rate is reduced from 16.51 to 10. For the splash image , the error rate is reduced from 1.5 to 0.

V. CONCLUSION AND FUTURE ENHANCEMENT

For providing an efficient way of sending data inside an image, a reversible data hiding using side match is adopted. The security provided in the earlier works of stenography and cryptography including the Zhang's work did not fully exploit the pixels in calculating the smoothness of each block and did not consider the pixel correlations in the border of neighbouring blocks. These two issues could reduce the correctness of data extraction. This work adopts a better scheme for measuring the smoothness of blocks, and uses the side-match scheme to further decrease the error rate of extracted-bits. The experimental results reveal that the proposed method offers better performance over Zhang's work. For example, when the block size is set to 8x8, the error rate of the Lena image of the proposed method is 0.34%, which is significantly lower than 1.21% of Zhang's work. Many reversible data hiding methods have been proposed recently embeds data bits by expanding the difference of two consecutive pixels. It uses a lossless compression technique to create extra spaces for carry data bits and shifts the bins of image histograms to leave an empty bin for data embedment adopts the difference expansion and histogram shifting for data embedment. It then embeds data by shifting the histogram of prediction errors while considering the local activity of pixels to further enhance the quality of stegoimage. There are also a number of works on data hiding in the encrypted domain. In a buyer–seller watermarking protocol the seller of digital multimedia product encrypts the original data using a public key, and then permutes and embeds an encrypted fingerprint provided by the buyer in the encrypted domain.

In another type of joint data-hiding and encryption schemes, a part of cover data is used to carry the additional message and the rest of the data are encrypted, so that both the copyright and the privacy can be protected. For example the intra prediction mode, motion vector difference and signs of DCT coefficients are encrypted, while a watermark is embedded into the amplitudes of DCT coefficients. In the cover data in higher and lower bit-planes of transform domain marked. In the content owner encrypts the signs of host DCT coefficients and each content-user uses a different key to decrypt only a subset of the coefficients, so that a series of versions containing different fingerprints are generated for the users.

REFERENCES

[1] Wien Hong, Tung-Shou Chen, and Han-Yan Wu "An Improved Reversible Data Hiding in Encrypted Images Using Side Match", IEEE SIGNAL PROCESSING LETTERS, VOL. 19, NO. 4, APRIL 2012
[2] Udayakumar R., Khanaa V., Saravanan T., "Analysis of polarization mode dispersion in fibers and its mitigation using an optical compensation technique", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4767-4771.
[3] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su, "Reversible data hiding", IEEE Trans. Circuits And Systems For Video Technology., vol.16, no.3, pp.354-362, 2008.
[4] Mahalakshmi K., Prabhakar J., Sukumaran V.G., "Antibacterial activity of Triphala, GTP & Curcumin on Enterococci faecalis", Biomedicine, ISSN : 0970 2067, 26(Mar-4) (2012) pp. 43-46.
[5] Jun Tian, "Reversible Data Embedding Using a Difference Expansion", IEEE Trans. Circuits and Systems for Video Technology., vol.13, no.8, 2006.
[6] Udayakumar R., Khanaa V., Saravanan T., "Chromatic dispersion compensation in optical fiber communication system and its simulation", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4762-4766.
[7] Xinpeng Zhang, "Reversible Data Hiding In Encrypted Image", IEEE Signal Processing Letters, vol.18, no.4, april 2011.
[8] Bhuvaneswari B., Hari R., Vasuki R., Suguna, "Antioxidant and antihepatotoxic activities of ethanolic extract of Solanum torvum", Asian Journal of Pharmaceutical and Clinical Research, ISSN : 0974-2441, 5(S3) (2012) pp. 147-150.
[9] Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image", IEEE Trans. On Information Forensics And Security, vol.7, no.2, 2012.
[10] Sathyanarayana H.P., Premkumar S., Manjula W.S., "Assessment of maximum voluntary bite force in adults with normal occlusion and different types of malocclusions", Journal of Contemporary Dental Practice, ISSN : 1526-3711, 13(4) (2012) pp.534-538.
[11] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, 2005.
[12] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," IEEE Trans. Image Process., vol. 16, no. 3,pp. 721–730, 2007.
[13] D.Kundur and K.Karthik, "Video fingerprinting and encryption principles for digital rights management," *Proc. IEEE*, vol. 92, pp. 918–932, 2004.
[14] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and Watermarking in video compression," IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, 2007.
[15] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and Neri, "A commutative digital image watermarking and encryption Method in the tree structured hard transform domain," Signal Process Image Commun., vol. 26, no. 1, pp. 1–12, 2011.
[16] Dr.K.P.Kaliyamurthie, D.Parameswari, Load Balancing in Structured Peer to Peer Systems, International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2249-2615,pp 22-26, Volume1 Issue 1 Number2-Aug 2011

[17] Dr.R.Udayakumar, Addressing the Contract Issue,Standardisation for QOS, International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Online): 2320 – 9801,pp 536-541, Vol. 1, Issue 3, May 2013

[18] Dr.R.Udayakumar, Computational Modeling of the StrengthEvolution During Processing And Service Of9-12% Cr Steels, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 3295-3302, Vol. 2, Issue 3, March 2014

[19] P.Gayathri, Assorted Periodic Patterns Intime Series Database Usingmining, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801, pp 5046- 5051, Vol. 2, Issue 7, July 2014.

[20] Gayathri, Massive Querying For Optimizing Cost – CachingService in Cloud Data, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 2041-2048, Vol. 1, Issue 9, November 2013