Steganography
Technique of Sending Random Passwords on Receiver's Mobile
(A New Technique to Hide Information File with an Image)

Shubhendu S. Shukla[1], Vijay Jaiswal[2], Sumeet Gupta[3], Anurag Singh[4]
[1](Asst. Professor/ Department of Management/ SR Group of Institutions, Lucknow)
[2](Asst. Professor/ Department of Information Technology/ SR Group of Institutions, Lucknow)
[3](Asst. Professor/ Department of Computer Science/ SR Group of Institutions, Lucknow)
[4](Asst. Professor/ Department of Computer Science / SR Group of Institutions, Lucknow)

Abstract: *Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. There are many application of Steganography with different carrier file format. Here we perform Steganography Technique with sending OTP on receiver mobile, which is one of the best secured technique in current scenario. This technique is hiding file information into image with OTP password that is only known by receiver. And can decrypt using that OTP only this is pure Steganography. Pure Steganography means that there is none prior information shared by two communication parties. We are not sharing OTP information by two communication parties. So this is more secure than other technique.*

Key Words : *Steganography, OTP, ICT, Password, IP, UDP, SIHS, LSB.*

I. Introduction

One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of Steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists.

Steganography become more important as more people join the cyberspace revolution. Steganography is the art of concealing information in ways that prevents the detection of hidden messages. Steganography include an array of secret communication methods that hide the message from being seen or discovered.

Due to advances in ICT, most of information is kept electronically. Consequently, the security of information has become a fundamental issue. Besides cryptography, Steganography can be employed to secure information. In cryptography, the message or encrypted message is embedded in a digital host before passing it through the network, thus the existence of the message is unknown. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video and images.

The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the internet increases. Therefore, the confidentiality and data integrity are requires to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and Steganography.

Steganography hide the secrete message within the host data set and presence imperceptible and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an information analysis.

II. What is Steganography?

- Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out to the usual. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between two is that Steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information.
- What Steganography essentially does is exploit human perception, human senses are not trained to look for files that have information inside of them, although this software is available that can do what is called Steganography. The most common use of Steganography is to hide a file inside another file.

III. History of Steganography:

Through out history Steganography has been used to secretly communicate information between people. Some examples of use of Steganography is past times are:

During World War 2 invisible ink was used to write information on pieces of paper so that the paper appeared to the average person as just being blank pieces of paper. Liquids such as milk, vinegar and fruit juices were used, because when each one of these substances are heated they darken and become visible to the human eye.

In Ancient Greece they used to select messengers and shave their head, they would then write a message on their head. Once the message had been written the hair was allowed to grow back. After the hair grew back the messenger was sent to deliver the message, the recipient would shave off the messengers hair to see the secrete message.

IV. Project Scope:

This paper is developed for hiding information in any image file. The scope of the paper is implementation of Steganography tools for hiding information includes any type of information file and image files and the path where the user wants to save Image and extruded file.

V. Methodology:

User needs to run the application. The user has two tab options – encrypt and decrypt. If user select encrypt, application give the screen to select image file, information file and option to save the image file. If user select decrypt, application gives the screen to select only image file and ask path where user want to save the secrete file.

This project has two methods – Encrypt and Decrypt.

- In encryption the secrete information is hiding in with any type of image file.
- Decryption is getting the secrete information from image file.

VI. Steganography vs Cryptography:

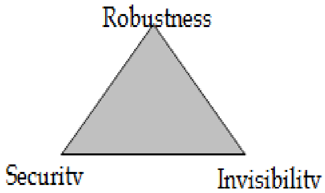
Basically, the purpose of cryptography and Steganography is to provide secret communication. However, Steganography is not the same as cryptography. Cryptography hides the contents of a secrete message from a malicious people, whereas Steganography even conceal the existence of the message. In cryptography, the system is broken when the attacker can read the secret message. Breaking a Steganography system need the attacker to detect that Steganography has been used.

It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using Steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged.

VII. Steganography vs Watermarking:

Steganography pay attention to the degree of Invisibility while watermarking pay most of its attribute to the robustness of the message and its ability to withstand attacks of removal, such as image operations(rotation, cropping, filtering), audio operations(rerecording, filtering)in the case of images and audio files being watermarked respectively.

It is a non-questionable fact that delectability of a vessel with an introduced data (Steganography message or a watermark) is a function of the changeability function of the algorithm over the vessel.



That is the way the algorithm changes the vessel and the severity of such an operation determines with no doubt the delectability of the message, since delectability is a function of file characteristics deviation from the norm, embedding operation attitude and change severity of such change decides vessel file delectability.

A typical triangle of conflict is message Invisibility, Robustness, and Security. Invisibility is a measure of the in notability of the contents of the message within the vessel.

Security is sinominous to the cryptographic idea to message security, meaning inability of reconstruction of the message without the proper secret key material shared.

Robustness refers to the endurance capability of the message to survive distortion or removal attacks intact. It is often used in the watermarking field since watermarking seeks the persistence of the watermark over attacks, steganographic messages on the other hand tend to be of high sensitivity to such attacks. The more invisible the message is the less secure it is (cryptography needs space) and the less robust it is (no error checking/recovery introduced).The more robust the message is embedded the more size it requires and the more visible it is.

VIII. Applications of Steganography

Steganography is applicable to, but not limited to, the following areas.

- Confidential communication and secret data storing
- Protection of data alteration
- Access control system for digital content distribution
- Media Database systems

The area differs in what feature of the Steganography is utilized in each system.

8.1. Legitimate Use

Steganographic techniques have obvious uses, some legitimate, some less so, and some are likely illegal. The business case for protection of property, real and intellectual is strong. The watermarking of digital media is constantly improving, primarily in an attempt to provide hardened watermarks or proof of ownership.
Individuals or organizations may decide to place personal/private/sensitive information in Steganographic carriers. Admittedly, there are usually better ways to manage this task. One can liken these applications to the use of a deadbolt lock on a door. The deadbolt will keep honest people honest, but those determined to break and enter can simply break a window and gain entry. With advances in Steganography, it is possible that this medium could serve as a relatively secure storage/transmission method.

8.2. Illegal Use

Other uses for Steganography range from the trivial to the abhorrent. There are claims that child pornography may be lurking inside innocent image or sound files. While this is entirely possible, a search on the internet for confirmation of this claim was unsuccessful.
An annual report on High Technology crime lists nine common types of computer crime:

- Criminal communications
- Fraud
- Hacking
- Electronic payments
- Gambling and pornography
- Harassment
- Intellectual property offenses
- Viruses
- Pedophilia

In examining this list, one can identify several of these areas where Steganography could be used, especially considering the broad term "criminal communications." If one includes Steganographic techniques other than computer related, the potential grows even more.

In terms of computer security, there are some areas to be aware of. One area that has potential far ranging implications is "A protocol that uses Steganography to circumvent network level censorship." The author, Bennet Haselton, the coordinator of Peacefire.org (an organization that "opposes censorship that targets Internet users under 18…") describes a protocol that is "undetectable to censors."
Finally, computer warfare should be addressed. In his Masters Thesis, Jordan T. Cochran, Captain, USAF investigates Steganographic virus attacks. He finds that "The results indicate that Steganography tools are not conducive to be sole attack weapons. However, the tools combined with other applications could be used to automatically extract the hidden information with minimal user intervention."

In another Masters Thesis, Dale A. Lathrop, Captain, USAF also investigates the possibility of virus attacks using Steganographic techniques. He finds that "The results of this research indicate that the use of a separate engine followed by an HTML-based electronic mail message containing a photographic image with a Steganographically embedded virus or other payload is a vulnerable attack if implemented without the proper environment variables in place." He further finds that "it still requires human intervention to initiate the virus attack."

For those who find themselves as first responders in electronic crimes, the "Electronic Crime Scene Investigation, A Guide for First Responders" written in July 2001 is freely available on the internet. This publication offers basic, sound advice in the preservation and investigation of electronic crime scenes, and does give mention to Steganography.

IX. Future Enhancements, Future Considerations:

- To make it pure Steganography application with multiple password.
- Due to time and computing limitations, we cannot explore all facets of Steganography and detection techniques. As we studied the power in our pictures to test for hidden data. Another method which we were unable to explore was to analyze the noise of the pictures. Adding hidden data adds random noise, so it follows that a properly tuned noise detection algorithm could recognize whether or not a picture had Steganography data or not.

9.1. Future Steganography

According to Richard E. Smith (a data security expert), he doesn't "see many practical uses for Steganography because it only works as long as nobody expects you to use it." The author respectfully takes exception to this statement. Initially after reading this statement, the myth that Charles H. Duell, Commissioner of Patents in 1899 had declared that the Patent Office should be closed because everything that could possibly be invented had already been invented came to mind. Perhaps the computer security community should give up on endless patches, security applications, etc because they only work if nobody expects that they are in use. To quote Dale Carnegie, "Most of the important things in the world have been accomplished by people who have kept on trying when there seemed to be no hope at all."

There are ongoing studies to harden Steganographic images from steganalysis. In his paper, "Defending Against Statistical Steganalysis," Provos presents new methods which would allow one to select a file in which a message might be safely hidden and resistant to standard statistical analysis.

X. Objective

The goal of this Steganography system is to convert communication. So, a fundamental requirement of this Steganography system is that the hider message carried by Stego-media should not be sensible to human beings. The other goad of Steganography is to avoid drawing suspicion to the existence of a hidden message. This approach of information hiding technique has recently became important in a number of application area

This project has following objectives:

- To product security tool based on Steganography techniques.
- To explore techniques of hiding data using encryption module with more secure random password only known by receiver.
- To extract techniques of getting secret data using decryption module by authenticate user.
- Steganography sometimes is used when encryption is not permitted. Or, more commonly, Steganography is used to supplement encryption. An encrypted file may still hide information using Steganography, so even if the encrypted file is deciphered, the hidden message is not seen

XI. Overview

The word Steganography comes from the Greek "***Steganos***", which mean ***covered or secret*** and –"***graphy***" mean **writing or drawing**. Therefore, Steganography means, literally, covered writing. It is the art and science of hiding information such its presence cannot be detected and a communication is happening. A secrete information is encoding in a manner such that the very existence of the information is concealed. Paired with existing communication methods, Steganography can be used to carry out hidden exchanges. The main goal of this paper it to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hider data. There has been a rapid growth of interest in Steganography for two reasons:

The publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products

Moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages.

The basic model of Steganography consists of Carrier, Message and password. Carrier is also known as cover-object, which the message is embedded and serves to hide the presence of the message.

Basically, the model for Steganography is shown on following figure:

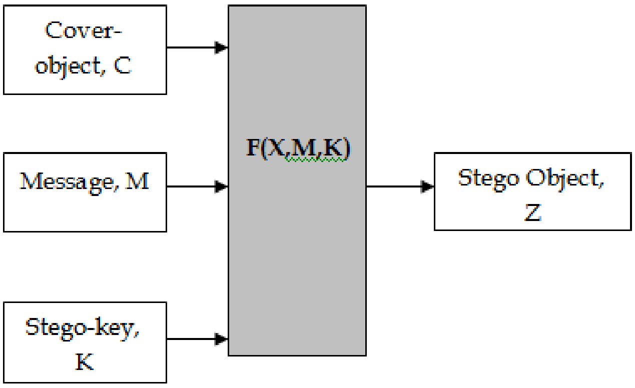


Figure 1 CONCEPT OF STEGANOGRAPHY

Message is the data that the sender wishes to remain it confidential. It can be plain text, cipher text, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. Password is known as *Stego-key*, which ensures that only recipient who knows the corresponding decoding key will be able to extract the message from a *cover-object*. The *cover-object* with the secretly embedded message is then called the *Stego-object*.

Recovering message from a *Stego-object* requires the *cover-object* itself and a corresponding decoding key if a *Stego-key* was used during the encoding process. The original image may or may not be required in most applications to extract the message. There are several suitable carriers below to be the *cover-object:*

- Network protocols such as TCP, IP and UDP
- Audio that using digital audio formats such as wav, midi, avi, mpeg, mpi and voc
- File and Disk that can hides and append files by using the slack space
- Text such as null characters, just alike morse code including html and java
- Images file such as bmp, gif and jpg, where they can be both color and gray-scale.
- In general, the information hiding process extracts redundant bits from *cover-object.* The process consists of two steps:
- Identification of redundant bits in a *cover-object.* Redundant bits are those bits that can be modified without corrupting the quality or destroying the integrity of the *cover-object.*
- Embedding process then selects the subset of the redundant bits to be replaced with data from a secret message. The *Stego-object* is created by replacing the selected redundant bits with message bits

XII. Requirements:

12.1. Software Requirements:

- .NET Framework 3.5

12.2. Hardware Requirements:

- Processor: Preferably 1.0 GHz or Greater.
- RAM : 1.0 GB or Greater.

XIII. Steganography Techniques:

Over the past few years, numerous Steganography techniques that embed hidden messages in multimedia objects have been proposed. There have been many techniques for hiding information or messages in images in such a manner that alteration made to the image is perceptually indiscernible. Commonly approaches are includes LSB, Masking and filtering and Transform techniques. Least significant bit (LSB) insertion is a simple approach to embedding information in image file. The simplest Steganography techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in human perceptible difference because the amplitude of the change is small. In this technique, the embedding capacity can be increased by using two or more least significant bits. At the same time, not only the risk of making the embedded message statistically detectable increase but also the image fidelity degrades. Hence a variable size LSB embedding schema is presented, in which the number of LSBs used for message embedding/extracting depends on the local characteristics of the pixel. The advantage of LSB-based method is easy to implement and high message pay-load.

Although LSB hides the message in such way that the humans do not perceive it, it is still possible for the opponent to retrieve the message due to the simplicity of the technique. Therefore, malicious people can easily try to extract the message from the beginning of the image if they are suspicious that there exists secret information that was embedded in the image.

Therefore, a system named Secure Information Hiding System (SIHS) is proposed to improve the LSB scheme. It overcomes the sequence-mapping problem by embedding the massage into a set of random pixels, which are scattered on the cover-image. Masking and filtering techniques, usually restricted to 24 bits and gray scale image, hide information by marking an image, in a manner similar to paper watermarks. The technique perform analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to cover image than just hiding it in the noise level.

Transform techniques embed the message by modulating coefficient in a transform domain, such as the Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other variant.

13.1. Image Steganography and bitmap pictures:

Using bitmap pictures for hiding secret information is one of most popular choices for Steganography. Many types of software built for this purpose, some of these software use password protection to encrypting information on picture. To use these software you must have a 'BMP' format of a pictures to use it, but using other type of pictures like "JPEG", "GIF" or any other types is rather or never used, because of algorithm of "BMP" pictures for Steganography is simple. Also we know that in the web most popular of image types are "JPEG" and other types not "BPM", so we should have a solution for this problem. This software provide the solution of this problem, it can accept any type of image to hide information file, but finally it give the only "BMP" image as an output that has hidden file inside it.

13.2. Bitmap Steganography:

Bitmap type is the simplest type of picture because that it doesn't have any technology for decreasing file size. Structure of these files is that a bitmap image created from pixels that any pixel created from three colors (Red, Green and Blue said RGB) each color of a pixel is one byte information that shows the density of that color. Merging these three colors makes every color that we see in these pictures. We know that every byte in computer science is created from 8 bit that first bit is Most-Significant-Bit (MSB) and last bit Least-Significant-Bit (LSB), the idea of using Steganography science is in this place; we use LSB bit for writing our security information inside BMP pictures. So if we just use last layer (8st layer) of information, we should change the last bit of pixels, in other hands we have 3 bits in each pixel so we have **3*hight*width** bits memory to write our information. But before writing our data we must write name of data (file), size of name of data & size of data. We can do this by assigning some first bits of memory (8st layer).

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Using each 3 pixel of picture to save a byte of data Difference between previous and current system graphical representation is as follows:

XIV. Previous System of Steganography :

Steganography system requires any type of image file and the information or message that is to be hidden. It has two modules encrypt and decrypt.

Microsoft .Net framework prepares a huge amount of tool and options for programmers that they simples programming. One of .Net tools for pictures and images is auto-converting most types of pictures to BMP format. I used this tool in this software called "Steganography" that is written in C#.Net language and you can use this software to hide your information in any type of pictures without any converting its format to BMP (software converts inside it).

The algorithm used for Encryption and Decryption in this application provides using several layers lieu of using only LSB layer of image. Writing data starts from last layer (8st or LSB layer); because significant of this layer is least and every upper layer has doubled significant from its down layer. So every step we go to upper layer image quality decreases and image retouching transpires.

The encrypt module is used to hide information into the image; no one can see that information or file. This module requires any type of image and message and gives the only one image file in destination.

The decrypt module is used to get the hidden information in an image file. It take the image file as an output, and give two file at destination folder, one is the same image file and another is the message file that is hidden it that.

Before encrypting file inside image we must save name and size of file in a definite place of image. We could save file name before file information in LSB layer and save file size and file name size in most right-down pixels of image. Writing this information is needed to retrieve file from encrypted image in decryption state. The graphical representation of this system is as follows:

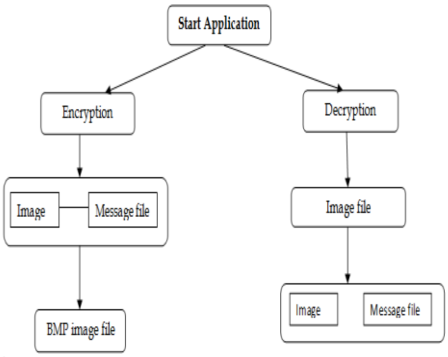


Figure 2 PREVIOUS SYSTEM OF STEGANOGRAPHY

14.1. Current System of Steganography:

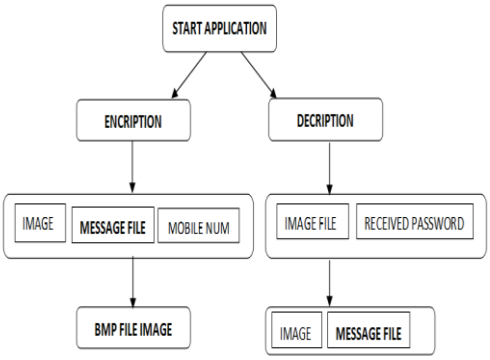


Figure 3 CURRENT SYSTEM OF STEGANOGRAPHY

XV. Limitations of the Software:

This paper has an assumption that is both the sender and receiver must have shared some secret information before imprisonment. Pure Steganography means that there is none prior information shared by two communication parties.

XVI. Conclusion:

Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day. Steganography can be used for hidden communication. We have explored the limits of Steganography theory and practice. We printed out the enhancement of the image Steganography system using LSB approach to provide a means of secure communication. A Stego-key has been applied to the system randomly by system during embedment of the message into the cover image. Stego-key is only known by receiver than remove the previous system drawback, because pure Steganography do not share any common information at both end sender and receiver.

This Steganography application software provided for the purpose to how to use any type of image formats to hiding any type of files inside their. The master work of this application is in supporting any type of pictures without need to convert to bitmap, and lower limitation on file size to hide, because of using maximum memory space in pictures to hide the file. Since ancient times, man has found a desire in the ability to communicate covertly. The recent explosion of research in watermarking to protect intellectual property is evidence that Steganography is not just limited to military or espionage applications. Steganography, like cryptography, will play an increasing role in the future of secure communication in the "digital world".

References

[1] "Information Hiding: A survey" (pdf). *Proceedings of the IEEE (special issue)* **87** (7): 1062–78. doi:10.1109/5.771065. Retrieved 2008-09-02.

[2] A New Text Steganography Method By Using Non-Printing Unicode Characters, Akbas E. Ali, Eng. & Tech. Journal, Vol.28, No.1, 2010

[3] B.r., Roshan Shetty; J., Rohith; V., Mukund; Honwade, Rohan; Rangaswamy, Shanta (2009). *Steganography Using Sudoku Puzzle*. pp. 623–626. doi:10.1109/ARTCom.2009.116.

[4] Chvarkova, Iryna; Tsikhanenka, Siarhei; Sadau, Vasili (15 February 2008). "Steganographic Data Embedding Security Schemes Classification". *Steganography: Digital Data Embedding Techniques*. Intelligent Systems Scientific Community, Belarus. Retrieved 25 March 2011.

[5] Johnson, Neil; Duric, Zoran; Jajodia, Sushil (2001). *Information hiding: steganography and watermarking: attacks and countermeasures*. Springer. ISBN 978-0-7923-7204-2.

[6] Krzysztof Szczypiorski (4 November 2003). "Steganography in TCP/IP Networks. State of the Art and a Proposal of a New System - HICCUPS". *Institute of Telecommunications Seminar*. Retrieved 17 June 2010.

[7] Kundur D. and Ahsan K. (April 2003). "Practical Internet Steganography: Data Hiding in IP". *Texas Wksp. Security of Information Systems*. Retrieved 16 June 2010.

[8] Vincent Chu. "ASCII Art Steganography".

WEBSITES :

[1] Computer steganography. Theory and practice with Mathcad (Rus) 2006 paper by Konakhovich G. F., Puzyrenko A. Yu. published in *MK-Press* Kyiv, Ukraine

[2] Detecting Steganographic Content on the Internet. 2002 paper by Niels Provos and Peter Honeyman published in *Proceedings of the Network and Distributed System Security Symposium* (San Diego, CA, February 6–8, 2002). NDSS 2002. Internet Society, Washington, D.C.

[3] Examples showing images hidden in other images

[4] File Format Extension Through Steganography by Blake W. Ford and Khosrow Kaikhah

[5] Information Hiding: Steganography & Digital Watermarking. Papers and information about steganography and steganalysis research from 1995 to the present. Includes Steganography Software Wiki list. Dr. Neil F. Johnson.

[6] Steganography at the Open Directory Project

Author's profile

Author[1] (Shubhendu S. Shukla), has completed his MA (Economics) in 2005 and MBA in 2007, and M.Phil (Management) in 2010. He has done Post Graduated Diploma in Computer Applications from IGNOU and Post Graduated Diploma in International Business from Annamalai University.

Author is Member of Editorial Board in Reviewer Panel of International Journal of Science and Research (IJSR) ISSN: 2319-7064 (www.ijsr.net/editorial.php), International Journal of Scientific Engineering and Research (IJSER) ISSN: 2614-7324 (www.ijser.in/members.php), International Journal of Engineering Research and Technology (IJERT) ISSN: 2278-0181, ISO 3297:2007 Certified Journal (http://www.ijert.org/about-us/review-board?start=9), International Journal of Modern Communication Technologies & Research (IJMCTR), ISSN : 2321-0850, An ISO 9001:2008 certified online journal http://erpublication.org/IJMCTR/Editorial%20Board.htm), Member of Editorial Board for Research Journali's^{TM} online journal, Journal of Human Resource (JHR) (http://researchjournali.com/join_editor.php).

He has worked with a prominent IT Company (Wipro Technologies) as Project Manager for e-Governance that was a Central Govt. Project about e-District, during his job he was responsible for Dealing with Consultant (Wipro), dealing with Techno team i.e. Trainer and other staff, he also Co-ordinate with District Administrative staff for monitoring, reporting, and his proposals and finally developed the Study materials.

Author has more than 6 years of experience in academics as he is currently working as Asst professor in SR Group of Institutions, Lucknow. With the academics author has publish 18 International Research Paper, 12 National Research Papers, attended 9 National Conferences and Seminars, 4 International Seminars. Apart from SR Group of Institutions, Lucknow, he is Guest and Visiting Faculty of Study Centers of Global Open University Nagaland, Karnataka State Open University, Sikkim Manipal University, Utter Pradesh Rajarshi Tandon University.

Author has taught variety of subjects as Marketing, Sales and Distribution, Production and Operation management, Computer Application in Management, System Analysis & Design and Software Engineering, Database Management System, Electronic Commerce (Specialized subjects of Information Technology).

Vijay Jaiswal[2] has completed B.Tech (Information Technology) in 2009 and perusing M.Tech. Author has worked with a prominent company (Tata Group) as a Software Engineer for more than 2 year. He has more than 2 years of experience in academics as he is currently working as Asst professor in SR Group of Institutions, Lucknow, Department of Information Technology. With the academics author has publish 2 International Research Paper, 3 national Research Papers, attended 2 National Conferences and Seminars, 1 International Seminars. Apart from SR Group of Institutions, Lucknow, he is Visiting Faculty of Study Centers of Karnataka State Open University, Sikkim Manipal University. He has taught subjects as Parallel Algorithm, DBMS, Object Oriented System, Web Technology, and Operating System.

Sumeet Gupta[3] has completed B.Tech (Computer Science) in 2008 and M.Tech in final stage. Author has more than 4 years of experience in academics as he is currently working as Asst professor in SR Group of Institutions, Lucknow, Department of Computer Science. With the academics author has publish 2 International Research Paper, 3 National Research Papers, attended 2 National Conferences and Seminars, 1 International Seminars. Apart from SR Group of Institutions, Lucknow, he is Visiting Faculty of Study Centers of Karnataka State Open University. He has taught subjects as Design Analysis of Algorithm, Compiler, Computer Concepts and Programming.

Anurag Singh[4] has completed B.Tech (Computer Science) in 2008 and M.Tech in final stage. Author has more than 5 years of experience in academics as he is currently working as Asst professor in SR Group of Institutions, Lucknow, Department of Computer Science. With the academics author has publish 2 International Research Paper, 3 National Research Papers, attended 2 National Conferences and Seminars, 1 International Seminars. Apart from SR Group of Institutions, Lucknow, he is Visiting Faculty of Study Centers of Sikkim Manipal University. He has taught subjects as Automata, Discreet Mathematics, Graph Theory.