www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 11 November, 2014 Page No. 9092-9097

Digital Image Steganography- Then, Now & Analysis of its Techniques

Pratik Shinde[1], Amrita Palmal[2],Rohan Singh[3]

[1]Ramrao Adik Institute of Technology, Department of Computer Engineering,
Nerul, Navi Mumbai, Maharashtra, India – 400706.
pratikshinde171193@gmail.com

[2]Ramrao Adik Institute of Technology, Department of Computer Engineering,
Nerul, Navi Mumbai, Maharashtra, India – 400706.
amrita23061992@gmail.com

[3]Ramrao Adik Institute of Technology, Department of Computer Engineering,
Nerul, Navi Mumbai, Maharashtra, India – 400706.
rohan.muz2@gmail.com

Abstract:*Steganography is a process of hiding/encrypting confidential data files into carrier/host files, and transmitting the obtained encrypted files from the sender to the receiver. It is the art of inconspicuously hiding data within data, so that unwanted recipients do not suspect and decipher the original, confidential message. Although people have employed the technique of hiding secret messages in plain sight using various novel techniques throughout ages, the recent surge in computer usage and technological advances has propelled the need for security and confidentiality to the forefront. Therefore, it is essential to develop an efficient tool which will incorporate all the security and confidentiality needs, and which shall withstand malicious intrusion attacks.It is important to understand that messages are not secure just by being hidden. Steganography is not all about keeping the messages hidden, but rather keeping their existence hidden. For this purpose, the report will discuss several useful algorithms, their implementation, their advantages and shortcomings, and more specifically, how these algorithms can be employed to develop highly effective steganography solutions concerning images as the carrier medium.*

Keywords: Steganography, cover-image, stego-image, embed, key, secret

1. Introduction

Use of Internet or the World Wide Web (www) has seen such a tremendous increase in the last decade that security and confidentiality of information has grown on to become one of the most important factors in information technology and communications. Every day, myriad of data is transmitted through the internet, by means of e-mail, social networking websites, file sharing websites and so on. As the number of users rise each day, the importance of security is increasing in prominence. The truculent and highly competitive nature of the computer industry forces the newly developed web services to open up to the market at a breakneck pace, leaving little to no time for auditing of system security. Also, the urgent need for labor causes the development services to be staffed with less experienced personnel, who may have little knowledge or training in security. These loopholes create an atmosphere in communication systems to be exploited, and malicious intruders leap onto this opportunity, creating a very unpleasant situation.

Steganographic techniques usually refer to methods wherein secret data is embedded into cover data in such a way that unwanted intruders cannot discern the existence of secret data. The main goal of image steganography is to hide secret images into readable but non-critical cover images.Steganography hides the secret message within the cover data set, and makes its existence imperceptible, reliably transmitting the file to the receiver. The cover data set is purposely corrupted, but in a covert way, to make it invisible to steganalysis-the process of decrypting the cover file, usually with malicious intentions.

2. History

Steganography has been in use for ages, and its applications can be traced back from 440 B.C.

2.1 Shaved Heads

This method was employed way back in 440 B.C. by Histiaeus, the then absolute ruler of Greece. He had the heads of his slaves shaved, and then tattooed important information on their naked scalps. Then, their hair were allowed to grow, upon which the slaves were sent to the recipient. The receiver then shaved their heads again, and the secret message was revealed.

2.2 Wax Tablets

In ancient Greece, wax tablets, made of wood, and covered with a wax layer were used for concealing of a secret message. People wrote secret messages on the wooden tablet, then covered it with a wax coat, and then, over this coat, an innocent and straight-forward message was written to evade suspicion.

2.3 Invisible Inks

Usage of invisible inks was another effective method commonly used during World War II by the French authorities. Invisible inks were used for writing secret messages on the back of couriers. These inks turned visible only on heating of the paper. Fruit juice extracts, vinegar and milk were commonly used as invisible inks.

2.4 Microdots

During World War II, detective and espionage agents used photographically produced microdots- dots which were usually minute, typically smaller than the size of the period on a typewriter. These dots were used to send information from the sender to receiver and vice-versa. These dots were embedded into the paper, and were covered with an adhesive material. This paper reflected upon falling of light over it, and consequently, the message was revealed by viewing against glancing light.

2.5 Morse code

Morse code, a technique wherein each character (letter or numeral) is represented by a unique sequence of dots and dashes, was used for transmitting secret messages. The messages were written on the knitting yarn, using which a cloth was made and worn by the carrier. Morse code technique was also employed by Jeremiah Denton, a Rear Admiral and Naval Aviator in the United States Navy. He used this technique in a television conference to spell the word "TORTURE" by blinking his eyes in the Morse code pattern, informing the US military that Americans were being tortured in Northern Vietnam.

3. Background

3.1 Framework

Any steganography framework can be understood with the help of Figure 1. For any algorithm employing a stego-key, the encryption process generates a stego-image for any given cover image. In the decryption process, the same shared stego-key is used, and the inverse algorithm is applied to extract the hidden message from the stego-image. This framework can be well understood by illustrating "ThePrisoners' Problem" documented G.J Simmons [9]. In this problem, Austin and Brian are two jail inmates, who wish to communicate with each other so that they can plot a plan to escape from the prison. However, their communication is closely monitored by the supervisor, Jane. To transmit the secret message to Brian, Austin comes up with a plan. He embeds the secret message 'M' into a cover object 'C', ultimately producing stego-object 'S'. This object is then sent by Austin to Brian through the public channel. In an ideal steganography framework, the technique which is used for embedding of the secret message into the cover object is unknown to Jane, and hence, the secret is shared only between Austin and Brian. In private-key steganography,a secret key, which is used to embed the message is shared between Austin and Brian. This key may be a password, which is used as a seed to generate pseudo-random number in order to select pixel locations in the cover image for embedding the secret message. Jane has no knowledge about this key, although she may know of the method that Austin and Brian are using. In public key steganography, Austin and Brian have a private-public or vice-versa key pairs, and know each other's public key. A secret key, which is used to embed the message is shared between Austin and Brian.

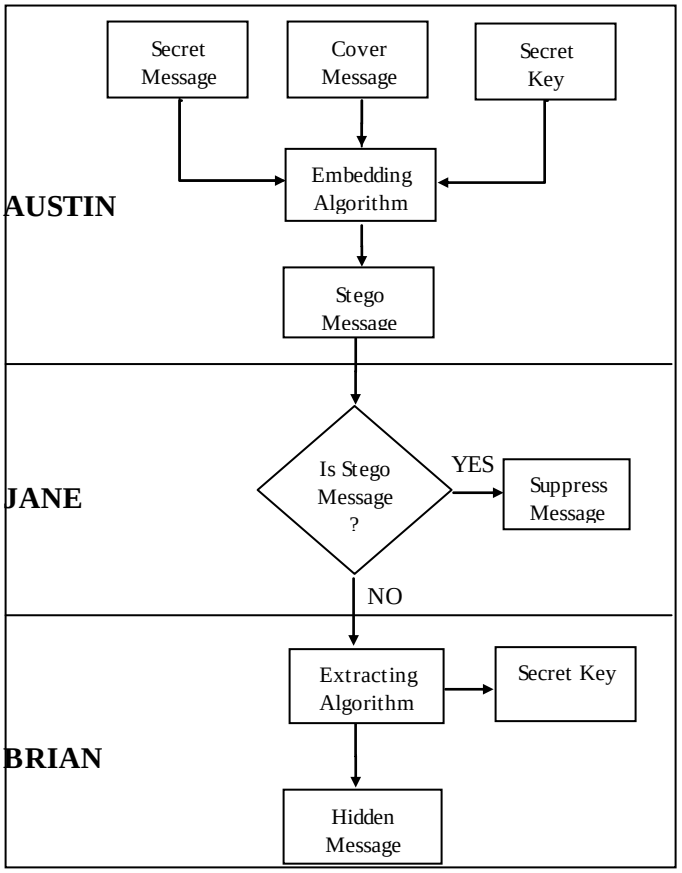

Figure 1: The Prisoners' Problem illustrating Steganography Framework

3.2 Steganography vs Cryptography

Steganography and Cryptography are closely related concepts. While Cryptography is derived from the Greek word *kryptos* which means 'hidden', Steganography is derived from the Greek word*steganos*which means 'covered, protected, or concealed'. The differences based on various properties are further illustrated in the table below:

Table 1: Steganography vs Cryptography

Properties	*Steganography*	*Cryptography*
Carrier &Payload,	Payload is embedded in any digital media file of any format(text, image,audio,video)	Payload is embedded in only text or image file format
Usage ofa secret key	Usage of secret key is optional; however it is recommended for better security and confidentiality.	Usage of secret key is compulsory for effective working of cryptographic algorithms.
Output file	The output file obtained after the embedding process is called a 'Stego-file', which contains the secret data hiding behind a cover file.	The output file obtained after the embedding process is called a 'Cipher-text', which contains the original file in an indiscernible form; hence the file is visible to everyone, but is not understandable.
Goal of the process	The goal of a secure steganographic algorithm is to prevent an intruder from obtaining knowledge of the mere presence of the secret data.	The goal of a secure cryptographic algorithm is to prevent an intruder from obtaining knowledge about the plaintext from the intercepted cipher-text.
User access to the output files	Only the sender and the receiver have access to the output files, via the use of a shared key, thus providing better data integrity.	Any person has access to the output files, hence any person can detect and modify the encrypted files, thus compromising on data integrity.
Attacks	Effective steganalysis leads to the detection of the presence of information.	Effective cryptanalysis deciphers the ciphered/encrypted information.
Visibility of operation	Information is not generally related to the cover file, and hence, is generally not perceptible to normal human vision.	Due to encryption, normal human vision detects the presence of hidden data; however deciphering is difficult.

3.3 Commonly used Terminologies

In order to understand how the process of steganography is carried out, it is important to know the following terminologies:

a) **Cover-Image**: This image is the image wherein the secret data is to be embedded. The term "cover" is usually used to describe the original and innocent nature of the file (text, image, audio, or video). The cover file is also referred to as the "host".

b) **Redundant Data**: This data usually constitutes certain pieces of information inside an image file which are simply unnecessary or irrelevant. Overwriting or altering of this data does not usually affect the quality of the original image. Generally, the least significant bits (LSB) of each pixel within an image are referred to as "Redundant" bits.

c) **Stego-Image:** This is the image wherein the actual secret information is hidden, along with the redundant data. That is, secret message + redundant data = Stego-image.The process of hiding secret information within the cover image is called as embedding.

d) **Payload:**Payload is the actual information or the secret data which is the primary concealment target. That is, Stego-image – cover-image = Payload. The data which is to be concealed within the cover image is known as the embedded data.

e) **Secret key:** This is the key which is used for user authentication, and to verify that the user has been granted access rights to read, modify or delete the contents of the stego-image. As a result, it keeps malicious intruders away from the secret data, hence providing security, confidentiality and integrity. It works as a password to encrypt or decrypt the cover-image and stego-image at the sender's and receiver's end respectively in order to embed or extract the payload.

f) **Steganalysis**: This is the process of attempting to break the steganography algorithm, and gain unwarranted access to the confidential data, without proper user access rights. This process is generally carried out by malicious intruders or hackers, who try to gain access to highly confidential data. Hence, it becomes all the more necessary to design a strong, reliable and secure algorithm, which will provide security to the concealed data, and will keep unwanted people away from it.

3.4 Working

The block diagram illustrated in Figure 2, adequately demonstrates the complete procedure of image steganography. A piece of data called the secret data is communicated between two authorized users- a sender and a receiver. A secret key is used for encryption and decryption of the secret data in order to establish safety and security and to maintain confidentiality of the data between the sender and the receiver. The usage of this key reduces the risk of malicious intrusion and hacking of the data or any third party attacks.

Firstly, the redundant data of the cover-image is extracted(for example, LSB of each pixel in an image file). Then this redundant data is substituted by the secret message with the help of some encryption algorithm. This results in the formation of a new image, called the stego-image, which contains the cover image along with the concealed data. A key(usually a combination of alphabets or numbers) is used during encryption to provide security to the confidential data. This key along with the stego-image is sent to the receiver via a communication channel. After receiving the stego-image, it is decoded using some decryption algorithm, and with the help of the key, the secret data is separated from the cover-image and this data is securely accessed by the receiver.

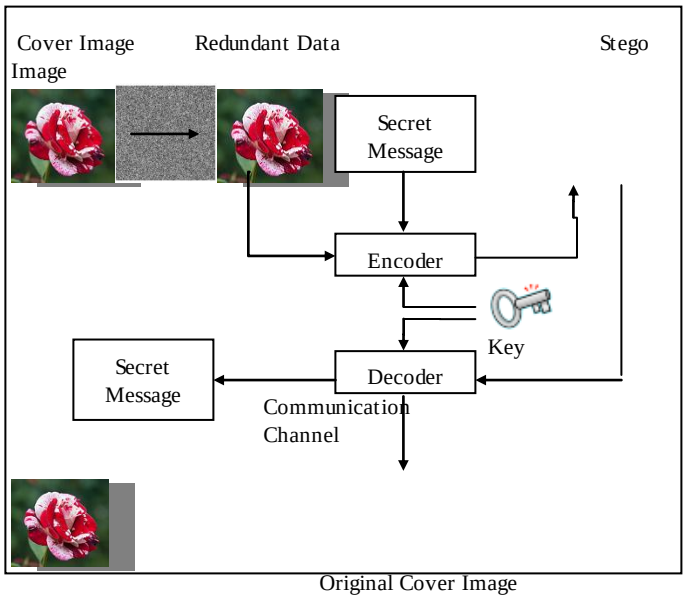

Figure 2: Block Diagram of Steganography

4. Implementation Techniques

Digital images of various formats are used as the carrier files in Image Steganography. The digital image can be compressed using either Lossy compression technique or Lossless compression technique. The former technique creates smaller files out of the original files by eliminating excess redundant data, thereby losing some image information. The most widely used image format in Lossy compression is JPEG (Joint Photographic Expert Group). On the other hand, Lossless compression performs certain formula based mathematical calculations to carry out compression, thereby resulting in little to no loss of data during the compression process. BMP (Bit Map) and GIF (Graphical Image Format) are two of the more commonly used image formats that undergo Lossless compression.

Various algorithms and techniques employing different ways of implementing steganography have been developed over the years. Some of the more commonly used algorithms are illustrated in Figure 3 as follows:

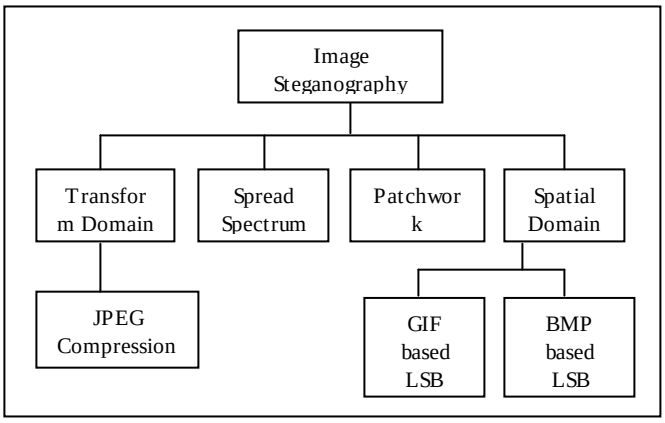

Figure 3: Common Steganography Techniques

4.1 JPEG File Compression

The JPEG file compression technique is probably the most popular method used to implement steganography. This file format, as defined by Joint Photographic Experts Group stores the data present in the image as quantized frequency coefficients in a lossy compressed form. Figure 4 shows the complete working of this technique.

Firstly, the JPEG compressor takes an uncompressed bitmap image as the input. Then, it slices this image into parts of 8 by 8 pixels. Then, DCT transforms each block of pixels into DCT coefficients. The results obtained after this transformation are scaled according to a standard quantization table (Q-Table), which is a matrix that consists of 64 DCT coefficients. Then, an encryption algorithm is used in order to protect the confidential message. This message, after encryption is called a secret message such that $\overline{S} = \{s_1, s_2, s_3, \ldots, s_n\}$, wherein s_i is one secret message bit. Now, s_i is embedded into Least Significant Bit (LSB) of quantized DCT coefficients in a zig-zag scan order. After the secret bits are embedded in each block, Huffman coding, Run-length coding (RLC) and Differential Pulse Code Modulation (DPCM) of Entropy coding are used to compress each block, with the help of coding tables (C-Table). Finally, a JPEG stego-image is obtained, which consists of the secret message hidden within it.

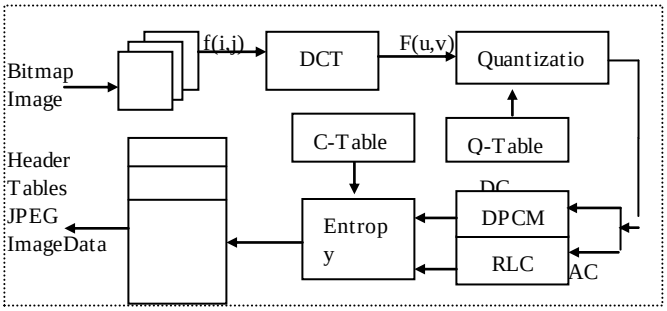

Figure 4:JPEG Steganography

4.2 Spread Spectrum

This technique is popularly known as SSIS (Spread Spectrum Image Steganography). Here, the secret data is interpreted as a

set of signals of narrowband frequencies that are scattered over a wideband of frequencies, called White noise or Gaussian noise. This noise is used to hide the secret data within it and after combining it with the cover-image, Stego-image is obtained. The hidden message can be obtained back at the receiver's end by making use of appropriate keys, without prior knowledge of the original image. This technique hides and extracts the secret message of substantial length along with maintaining original size and dynamic range of the original image. The power of the cover signal is very low when compared with the power of the cover signal. Hence, the secret message becomes imperceptible to normal human vision.This technique is generally used in covert communications, authentication, image tamper proofing, revision tracking and in-band captioning.

4.3 Patchwork

The Patchwork technique uses redundant pattern encoding method to hide the secret data into the cover image. Here, redundancy is achieved by adding a specific statistic along with a Gaussian distribution extrinsically to the cover-image, upon which the bits are scattered throughout the cover image. Consider two patches of the same image, say, Patch A and Patch B. Here, the algorithm works by slightly lightening the pixels in patch A, while darkening pixels in patch B. A pseudo-random number generator is used to determine the pixels that are to be lightened or darkened. A secret key is shared at the sender's and receiver's end which contains information of the modified pixels, thereby helping to encode or decode the secret message. The main disadvantage of this method is that it encodes only one bit at a time. However, more bits can be encoded by dividing the entire cover image into sub-images. The advantage of this technique is that even if one patch of the image is suppressed, other patches still exist. Hence, the entire data is not lost at a time.

4.4 Spatial domain

This technique employs the method of embedding the secret message into the intensity of the pixels directly. Here, unlike in JPEG compression, images are compressed using lossless data compression. The algorithm is dependent on the image format which is to be used as cover, and hence it can be broadly classified into two types- GIF based LSB & BMP based LSB.

4.4.1 LSB algorithm overview

A normal digitized image consists of a matrix consisting of color and intensity values. For a regular grey-scale image, 8 bits per pixel are used. Similarly, for a regular full-color image, 24 bits per pixel are used, wherein 8 bits are assigned to each color components - Red, Green and Blue (RGB).
LSB data insertion algorithm is a simple, widely used approach for embedding confidential information into a cover image. When using an 8-bit image, the 8th bit of some or all of the pixels inside an image is replaced with one bit of the secret message. Similarly, when using a 24-bit image, every 8th bit of each color component, namely Red, Green and Blue is replaced with one bit of the secret message. Hence, 3 bits of information can be stored in each pixel for a 24-bit image. According to this logic, in an 800 x 600 pixel image, a total of 1440000 bits or 180000 bytes of secret data can be embedded by replacing it with the LSB's of each pixel.

Moreover, since each primary color has 256 possible intensities, any change in a pixel results in minute changes in the intensity of that respective color. However, these changes are so miniscule that they are generally not perceptible to normal human vision. Therefore, by choosing a wise image, one can hide the secret message not only in the least significant bit, but also in the second to least significant bit, and still not notice any major difference.

A more secure LSB system can be implemented by employing a secret key that can be shared between the sender and the receiver, consisting details of only those pixels that are modified. Now, even if an intruder suspects that LSB steganography has been used, he does not own the key, and hence does not know which exact pixels have been modified and therefore has no start point.

The primary advantage of LSB steganography is its simplicity of use, and more space to occupy larger payload, in case of a BMP image. However, there are substantial disadvantages to this technique. LSB method is extremely sensitive to filtering or manipulation of the stego-image. Destruction of the message is very common in case of scaling, cropping, rotation or noise addition of the stego-image. Moreover, the intruder can easily destroy the message by zeroing the entire LSB plane, causing very little visual changes to the modified stego-image.

4.4.2 GIF based LSB

The Graphics Interchange Format (GIF) is generally used for storing of multiple bitmaps in a single file for exchange between various platforms and different images. GIF was designed with the primary goal of allowing easy interchanging and viewing of image data which are stored on local or remote computers. GIF is made up of a series of packets of data called as 'blocks' and is read as a continuous stream of data, pixel by pixel.

GIF images are also used for implementing LSB steganography. This approach is also called as 'Palette based approach'. The main issue with this approach is that changes made to the LSB of the pixel could result in a totally different color, since the index of the color palette is transformed. Another weak point is that since GIF images have a bit depth of eight, the total amount of information that can be embedded is usually less. Moreover, GIF images are vulnerable to visual as well as statistical attacks, since the modifications done to the color palette leaves a clear trace on the image.

4.4.3 BMP based LSB

Bitmap (BMP) image format was introduced by Microsoft as a standard image format between users of the Windows OS. Gradually, its usage increased, and now, BMP images are supported across multiple operating systems. However, its usage has been on a decline lately. The main reason behind this decline is its large file size, which results from its poor compression techniques and large verbose file format. The large file size, is however an advantage in steganography, since large file sizes provide more number of LSB's, and hence, more data can be embedded into a BMP image.

A BMP image can be broken down into two main blocks, header and data. The header consists of 54 bytes and it can be broken down into two sub-blocks. These sub-blocks are referred to as Bitmap Header, and Bitmap Information. Images that are less than 16 bits have an additional sub-block called the Color Palette which exists within the Bitmap header.

Since BMP images are not widely used, transmission of such images through LSB steganography might evoke intruder's suspicion. When carrier files are images in steganography, these files are generally manipulated by changing one or more bits of pixels of the image. The secret message may be stored in the LSB of one color of the RGB palette, or in the parity bit of the entire RGB value. Since BMP images are very large in size, they are capable of embedding quite a large amount of data within them. BMP based LSB is most suitable for applications wherein the primary focus is on the amount of information to be transmitted rather than on the secrecy of that information.

5. Conclusion

In this thesis, we focused our research on understanding the concept of Steganography wherein digital images were used as the carrier files. Then, we read the peculiar ways in which Steganography was implemented in ancient times; a time when the term 'Steganography' was not even coined. Further, we analyzed the different techniques and algorithms with the help of which Image Steganography is being implemented today and listed their advantages and shortcomings. Hence, we conclude that in today's age, where Internet is gaining supremacy as a means of data transmission and information communication, it becomes necessary to understand, analyze and provide security, confidentiality and integrity of data. The concept of Steganography provides just the right balance of all these attributes, thus helping to boost reliable communication between the sender and the receiver.

6. References

[1] http://en.wikipedia.org/wiki/Steganography [Accessed: Nov. 5, 2014]

[2] http://en.wikipedia.org/wiki/Cryptography [Accessed: Nov. 5, 2014]

[3] N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," Computer,vol. 31, no. 2, 1998, pp. 26–34

[4] L. von Ahn and N. J. Hopper, "Public-key steganography," in Advances in Cryptology: Eurocrypt 2004 (C. Cachin and J. Camenisch, eds.), vol. 3027 of Lecture Notes in Computer Science, pp. 322–339, Springer, 2004.

[5] Namita Tiwari and Dr.Madhu Shandilya, —Evaluation of Various LSB based Methods of Image Steganography on GIF File Format, in International Journal of Computer Applications (0975 – 8887) Volume 6– No.2, September 2010

[6] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi, —Image Steganography Techniques: An Overview, in International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3) : 2012

[7] Rosziati Ibrahim & Teoh Suk Kuan—Steganography Algorithm to Hide Secret Message inside an Image, Computer Technology and Application 2 (2011) 102-108

[8] Babloo Saha and Shuchi Sharma, —Steganographic Techniques of Data Hiding using Digital Images, in Defence Science Journal, Vol. 62, No. 1, January 2012, pp. 11-18, 2012,

[9] G. J. Simmons, "The prisoners' problem and the subliminal channel," in Advances in Cryptology: Proceedings of Crypto 83 (D. Chaum, ed.), pp. 51–67, Plenum Press, 1984

[10] Chandramouli, R. and Memon, N.: Analysis of LSB Based Image Steganography Techniques. Proceedings of ICIP 2001 (CD version). Thessaloniki, Greece (2001)

[11] Eggers, J.J., Bäuml, R., and Girod, B.: A Communications Approach to Image Steganography. Proceedings of SPIE: Electronic Imaging 2002, Security and Watermarking of Multimedia Contents, Vol. 4675. San Jose, California (2002)

Author Profile

Pratik Shinde, a student pursuing Bachelors in Engineering (B.E.) in Computer Engineering from Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, Maharashtra, India.

Amrita Palmal, a student pursuing Bachelors in Engineering (B.E.) in Computer Engineering from Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, Maharashtra, India.

Rohan Singh, a student pursuing Bachelors in Engineering (B.E.) in Computer Engineering from Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, Maharashtra, India.