International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 7th Mar 2018. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-03

Title: **A SECURE IMAGE STEGANOGRAPHY WITH DATA ENCRYPTION**

Volume 08, Issue 03, Pages: 109–117.

Paper Authors

G. NAGA RAJU, DR. P.V.RAMA RAJU, K.C.S.SUBBARAJU,K.GOPI KRISHNA, K.DHAWAN PRASAD REDDY, M.D.V.VENKATA SAI
SRKR Engg college(A), Bhimavaram, India

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A SECURE IMAGE STEGANOGRAPHY WITH DATA ENCRYPTION

[1]G. NAGA RAJU, [2]DR. P.V.RAMA RAJU, [3]K.C.S.SUBBARAJU,[4] K.GOPI KRISHNA, [5]K.DHAWAN PRASAD REDDY, [6]M.D.V.VENKATA SAI
[1]Asst. Professor, Department of ECE, SRKR Engg college(A), Bhimavaram, India.
[2]Professor & HOD, Department of ECE, SRKR Engg college(A), Bhimavaram, India.
[3,4,5,6] B.E Students, Department of ECE, SRKR Engg college(A), Bhimavaram, India.

ABSTRACT: Now a days communication has became the basic need for every individual. Security of information has always been a major issue from past tomes to the present. Therefore from time to time researchers have developed many techniques to send data without revealing it to anyone other than the receiver. Steganography and Cryptography are one of those techniques. Steganography is a method of hiding secret messages into cover object while communication takes place between sender and receiver while cryptography is the science of coding and decoding messages. In this paper we proposed a new technique of steganography by using LSB insertion and RSA algorithm.LSB insertion method for message. If in any case the cipher text revealed from cover image, the intermediate person other than the receiver can't access the message as it in the cipher text until he know the secret key.

Keywords: Cryptography, RSA encryption/decryption, Steganography, LSB insertion

1.INTRODUCTION:

The basic need of every growing area in today's world is communication. Everyone wants to keep the inside information of work to be secret and safe. We use many insecure pathways in our daily life for transferring and sharing information using internet or telephonically, but at a certain level it's not safe. Steganography and Cryptography are two methods which could be used to share information in a concealed manner. Cryptography includes modification of a message in a way which could be in digesting or encrypted form guarded by an encryption key which is known by sender and receiver only and without using encryption key the message couldn't be accessed. But in cryptography it's always clear to intermediate person that the message is in encrypted form, whereas in steganography the secret message is made to hide in cover image so that it couldn't be clearer to any intermediate person that whether there is any message hidden in the information being shared. The cover image containing the secret message is then transferred to the recipient. The recipient is able to extract the message with the help of retrieving process and secret key provided by the sender. A basic model of the steganographic process with cryptography is illustrated in Fig. 1.

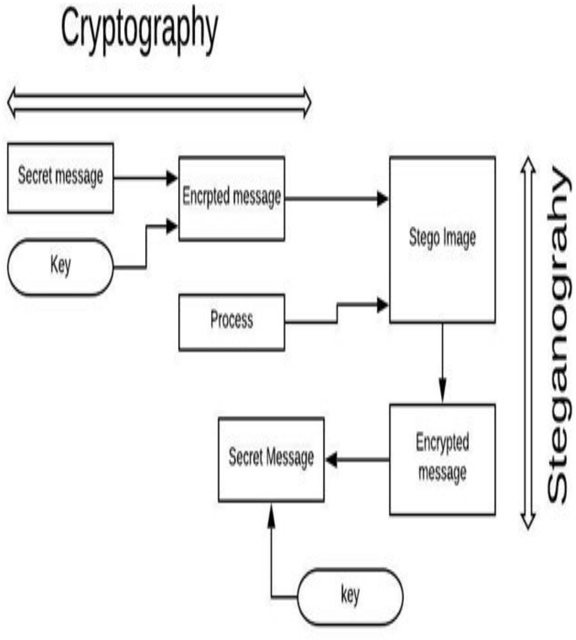


Fig1: A basic model of steganographic process with cryptography

1.1 CRYPTOGRAPHY

Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can be read and process it. The pre-fix “crypt” means “hidden” or ‘’vault” and the suffix ‘’graphy’’ stands for “writing”.

In Computer science ,cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule based calculations called algorithms to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation and digital signing and verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.[4]

Cryptographic techniques:

Cryptology is closely related to the disciplines of *cryptology* and *cryptanalysis* **.**It includes techniques such as microdots , merging words with images , and other ways to hide information in storage to transit. However, in today’s computer-centric world ,cryptography is most often associated with scrambling *plaintext***.**(ordinary text, sometimes referred to as clear text)into *cipher text* (a process called *encryption*),then back again (known as *decryption*).Individuals who participate this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:

a) Confidentiality: The information cannot be understood by anyone for whom it was unintended.

b) *Integrity:* The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected

c) *Non-repudiation*: the creator/ sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.

d) *Authentication*: the sender or receiver can confirm each others’ identity and the origin/ destination of the information.

1.2 STEGANOGRAPHY:

Steganography is a technique used to transmit a secret message from a sender to a receiver in a way such that a potential intruder does not suspect the existence of the message. Generally this can be done by embedding the secret message within another digital medium such as text, image, audio or video. [19]. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphie meaning "writing" [2]. The first recorded use of the term was in 1499 by Johannes Trithemius in his Stegano-graphia, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other "cover-text" and, classically, the hidden message may be in invisible ink between the visible lines of a private letter. It is a high security technique for long data transmission.

There are various methods of steganography[9]:

- Least significant bit (LSB) method
- Transform domain techniques
- Statistical methods
- Distortion techniques

2. RELATED WORK:

There are many ways to encrypt secret message(text).Of which RSA algorithm,Advanced Encryption algorithm are are more secure and widely used. Based on types of medium the secret message embedded steganography[] can be divided into text steganography[18] ,image steganography[23],[7],audio steganography [20] and video steganography [21]. In [18],Neha et.al, proposed a different methods in text Steganography. In [23],Alaa A.Jabbar et.al, proposed different techniques in image steganography. In [7],G.Naga Raju et.al, proposed a method to encrypt and decrypt a gray scale image using Advanced Encryption Standard(AES) algorithm. There are many steganography techniques which are capable of hiding data within an image. These techniques can be classified into two categories based on their algorithms: (1) spatial domain based techniques[11]; (2) transform domain based techniques [14]. The spatial domain based steganography[11] technique use either the LSB or Bit Plane Complexity Segmentation (BPCS) algorithm [22]. The most widely used technique to hide data is the usage of the LSB [6]. In [11], Dr.P.V Rama Raju et.al, proposed a paper based on pixel indicator method and LSB insertion which is combination of both BPCS and LSB-insertion where image is used as a key . In [14],Vaishali et.al , Propsed transform domain image steganography , which is one of the techniques used for hidden exanchange of data in frequency domain. In [22], Shrikant and DR.Sanjay proposed a bit plane complexity segmentation based steganography which increases the data data in an image to 50-60 % which is different from other BPCS steganography limited to 10-20%. The existing techniques are mainly based on LSB (Least Significant Bit) where LSBs of the cover file are directly changed with message bits. A significant number of methods have been proposed for LSB steganography like LSB steganography usin key [1], Robust Image Steganography [3], Hash Based LSB [19] and LSB binary addition method[17].Masud et al. [1] has proposed a LSB technique for RGB true color image by enhancing the existing LSB substitution techniques to improve the security level of hidden information. In [23] designing of robust and secure image steganography based on LSB insertion and RSA encryption technique has been used.In [18] two steganography technique proposed for hiding image in an image using LSB method for 24 bit color images. In [19] a hash based approach proposed for secure keyless steganography in lossless RGB images that an improved steganography approach for hiding text messages in lossless RGB images. In [17],G.Naga Raju et.al,proposed a technique of steganography in which secret data not directly embedded into cover image .The intensity of cover image pixel are adjusted in such a way that in the receiver side the actual target bits are extracted from stego file by performing binary addition. In [9], C.P.Sumathi et.al, propose a paper to analyse various techniques used in steganography and identified areas in which the techniques can be applied.In paper [7] proposes a secure covert communication model based on video steganography which is based on pixel-wise manipulation of colored raw video files to embed the secret data.

3. EXISTING TECHNIQUES USED:

There are a large number of cryptographic and steganographic methods that most of us are familiar with. The most widely used two techniques are:

- RSA algorithm
- Lsb Insertion method

3.1 RSA ALGORITHM

The algorithm was given by three MIT's Rivest, Shamir & Adleman and published in year 1977. RSA algorithm is a message encryption cryptosystem in which two prime numbers are taken initially and then the product of these values is used to create a public and a private key, which is further used in encryption and decryption. The RSA algorithm could be used in combination with LSB in a way that original text is embedded in the cover image in the form of cipher text. By using the RSA algorithm we are increasing the security to a level above. In case of steganalysis only cipher text could be extracted which is in the encrypted form and is not readable, therefore will be secure. RSA algorithm procedure can be illustrated in brief as follows [28]: the basic block diagram of RSA algorithm is shown in Fig2.

(i) Select two large strong prime numbers, p and q. Let n = p q.

(ii) Compute Euler's totient value for n: f (n) = (p - 1) (q - 1).

(iii) Find a random number e satisfying 1 < e < f (n) and relatively prime to f (n) i.e., gcd (e, f (n)) = 1.

(iv) Calculate a number d such that d = e-1 mod f (n).

(v) Encryption: Given a plain text m satisfying m < n, then the Cipher text c = m e mod n.

(vi) Decryption: The cipher text is decrypted by m = c d mod n

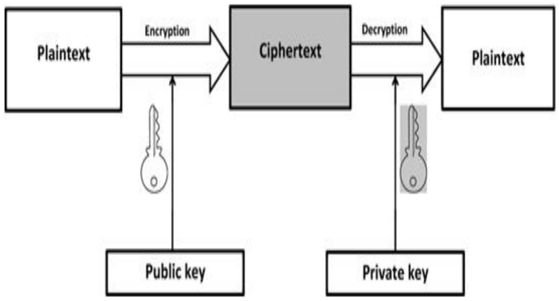
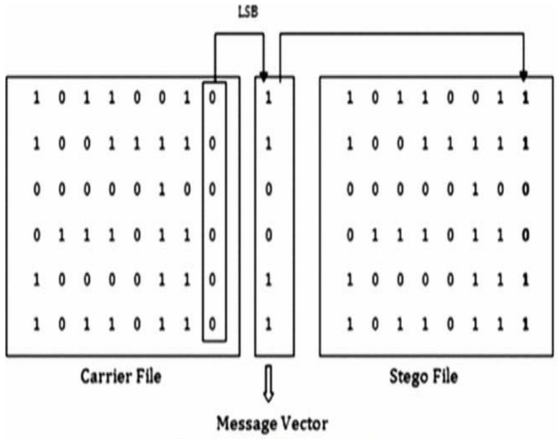


Fig2:RSA algorithm basic block diagram

3.2 LEAST SIGNIFICANT BIT (LSB) INSERTION METHOD:

One of the most common techniques used in steganography today is called least significant bit (LSB) insertion. Also called LSB (Least Significant Bit) substitution and it is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message into the image. In this method some information from the pixel of the carrier image is replaced with the message information so that it can't be observed by the human visual system, therefore it exploits some limitations of the human visual system. The Least Significant Bit insertion varies according to number of bits in an image . For an 8-bit image, the least significant bit i.e. the 8th bit of each byte of the image will be changed by the 1-bit of secret message. For 24 bit image, the colors of each component like RGB (red, green and blue) will be changed. LSB steganography involves the operation on least significant bits of cover image, audio or video. The least significant bit is the lowest bit in a series of binary number [16]. In LSB substitution the least significant bits of the pixels are displaced by the bits of the secret message which gives rise to an image with a secret message embedded in it. The method of embedding differs according to the number of bits in an image (different in 8 bit and 24 bit images). Basic LSB insertion with an example is as shown in Fig.3.



```
1 0 1 1 0 0 1 0    1    1 0 1 1 0 0 1 1
1 0 0 1 1 1 1 0    1    1 0 0 1 1 1 1 1
0 0 0 0 0 1 0 0    0    0 0 0 0 0 1 0 0
0 1 1 1 0 1 1 0    0    0 1 1 1 0 1 1 0
1 0 0 0 0 1 1 0    1    1 0 0 0 0 1 1 1
1 0 1 1 0 1 1 0    1    1 0 1 1 0 1 1 1
```

Fig3:Example of LSB insertion method

4. PROPOSED METHODOLOGY:

The problem statement consists of embedding the secret message in the LSB of each RGB pixels value of the cover image. Before embedding the secret message have to be converted to cipher text using RSA algorithm to enhance the secrecy of the message. In this approach we implemented a technique called LSB insertion on images. It is a challenging process which will lead us to combine the two technologies, one of them is RSA algorithm from cryptography and other is LSB insertion from steganography. Our research has focused on providing a solution for transferring and sharing important data without any compromise in security. All the reputed organizations while sending business documents over the internet always use encryption of the data to protect leakage of information about their organization from their rivals or intruders. We have used LSB insertion and RSA algorithm to create a secure steganography algorithm which is far more secure than many systems being used for the purpose of secretly sending the data.

4.1 Embedding Secret message in an Cover IMage

Step1: Cover Image and Secret Message:

In our proposed system, first of all we select a true color image and resize it to a size 512 x 512 for to it as a cover image and a secret message which is to be embed in the cover image.

Step2: Encryption of Secret Message:

The secret message has to be encrypted using RSA algorithm and convert into cipher text which is to be embed of cover image **.**

Step3: Least Significant bit process:

Now, We have to calculate the least significant bits (LSB) of cover Image where the bits of the message has to be embedded.

Step4: Embed cipher text into LSB of cover Image:

The cipher text obtained obtained after RSA encryption (4,step2) is to be embed in least significant bits of cover image (4,step 3) and get the stego-image which is to be send to the receiver A simple flow chart diagram of embedding algorithm is shown in in Fig4:

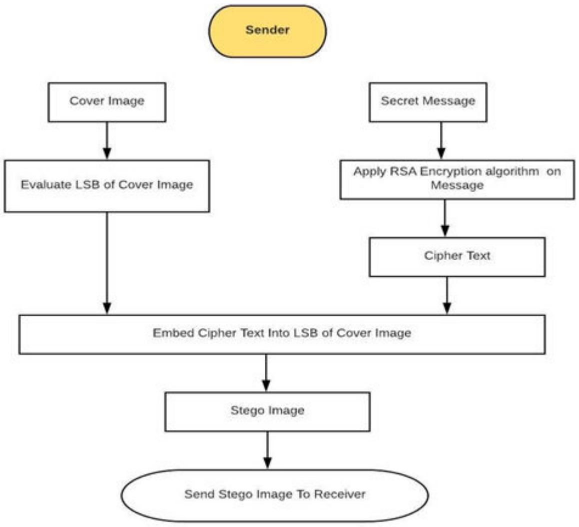

Sender
Cover Image
Secret Message
Evaluate LSB of Cover Image
Apply RSA Encryption algorithm on Message
Cipher Text
Embed Cipher Text Into LSB of Cover Image
Stego Image
Send Stego Image To Receiver

Fig4: Sender flow chart diagram get Stego image which is to be send to receiver

4.2 Getting Secret Image from Stego-Image Using LSB decoding and RSA decryption:

In the decoding process we have to detect the positions of the LSB's where the data bits had been embedded. When the position of the bits had been specified, the bits are then extracted from the position in the same order as they were embedded. At the end of this process we will get the message in binary form which again converted into decimal form, and with same process we got the cipher text message. After retrieving the positions of LSB's that contain secret data, the receiver will decrypt secret data using RSA algorithm. To apply RSA algorithm receiver will use his/her private key because the secret data have been encrypted by recipient public key. Using receiver private key cipher text will be converted into original message which is in readable form. A simple flow chart diagram in receiver is shown in fig5.

Retrieval Algorithm:

Step 1: Receive a stego image.

Step 2: Find 4 LSB bits of each RGB pixels from stego image.

Step 3: Apply hash function to get the position of LSB's with hidden data.

Step 4: Retrieve the bits using these positions in order of 3, 3, and 2 respectively.

Step 5: Apply RSA algorithm to decrypt the retrieved data.

Step 6: Finally read the secret message

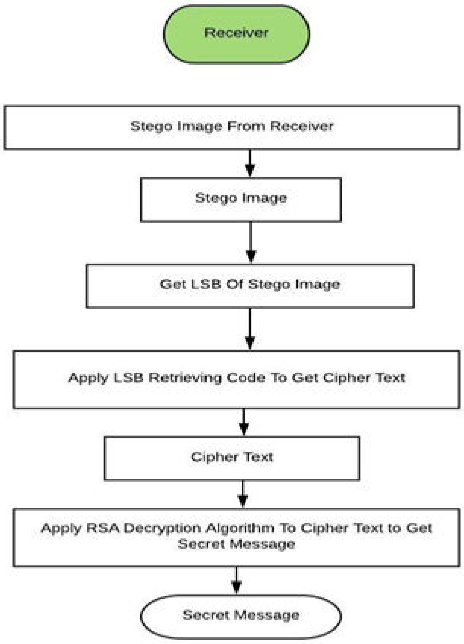

Receiver
Stego Image From Receiver
Stego Image
Get LSB Of Stego Image
Apply LSB Retrieving Code To Get Cipher Text
Cipher Text
Apply RSA Decryption Algorithm To Cipher Text to Get Secret Message
Secret Message

Fig5:Receiver flow chart diagram to get **secret message** from stego image.

V.RESULTS:

Example :

Implementation of RSA Algorithm

Enter value of p: 53

Enter value of q: 61

Initializing:

The value of (N) is: 3233

The public key (e) is: 7

The value of (Phi) is: 3120

The private key (d)is: 1783

Enter message: **SRKR engineering college ece**

ASCII Code of the entered Message:

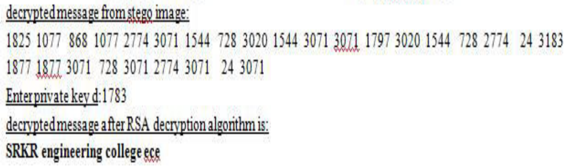
```
  Columns 1 through 20
 83    82    75    82    32   101   110   103
105   110   101   101   114   105   110   103
32   99   111   108
  Columns 21 through 28
  108   101   103   101    32   101    99   101
```

Cipher Text of the entered Message:

```
  Columns 1 through 10
      1825         1077          868         1077
2774        3071        1544         728        3020
1544
  Columns 11 through 20
       3071         3071         1797         3020
1544         728        2774          24        3183
1877
  Columns 21 through 28
       1877         3071          728         3071
2774        3071          24        3071
```

Fig6(a)original image

fig6(b)Stego image



decryptedmessage from stego image:

```
1825 1077  868 1077 2774 3071 1544  728 3020 1544 3071 3071 1797 3020 1544  728 2774  24 3183
1877 1877 3071  728 3071 2774 3071  24 3071
```

Enterprivate key d:1783

decryptedmessage after RSA decryption algorithm is:

SRKR engineering college ece

6. CONCLUSION:

A secured LSB technique for image steganography has been implemented. An efficient steganographic method for embedding secret messages into cover images without producing any major changes has been accomplished through this method. In this work, a new way of hiding information in an image with less variation in image bits have been created, which makes our technique secure and more efficient. This technique also applies a cryptographic method i.e. RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key. RSA algorithm itself is very secure that’s why we used in this technique to increase the security of the secret message. A specified embedding technique uses lsb insertion and also provide encryption of data uses RSA algorithm; makes our technique a very much usable and trustworthy to send information over any unsecure channel or internet. The future scope for the proposed method might be the development of an enhanced steganography that can have the authentication module along with encryption and decryption. Meanwhile the work can be enhanced for other data files like video, audio, text. Similarly the steganography technique can be developed for 3D images.

REFERENCES:

[1] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain “A New Approach for LSB Based Image Steganography using Secret Key”, International Conference on Computer and Information Technology (ICCIT), Pages No. 286 – 291, 22-24 Dec., 2011.

[2] Information about steganography available at https://en.wikipedia.org/wiki/Steganography

[3] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, “Steganography

Using Least Significant Bit Algorithm”, International Journal of Engineering Research and applications, vol.2, issue 3, pp. 338-341May-June2012

[3] Mamta Juneja, Parvinder Singh Sandhu, “Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption”, International Conference on Advances in Recent Technologies in Communication and Computing, Pages No. 302 – 305, 27-28 Oct., 2009.

[4] Information about cryptography, available at http://en.wikipedia.org/wiki/Cryptography.

[5] N. F. Johnson, S. Jajodia, "Steganography: seeing the unseen”, IEEE Computer, Vol. 31, Issue No. 2, Pages No. 26 - 34, Feb., 1998.

[6] Wien Hong, Tung-Shou Chen, “A Novel Data Embedding Method Using Adaptive Pixel Pair Matching”, IEEE Transactions on Information Forensics and Security, Vol. 7, Issue No. 1, Pages No. 176 - 184, Feb., 2012.

[7] G. Nagaraju,Dr. P V Ramaraju,RK Chaitanya,” Image Encryption and Decryption Using Advanced Encryption Algorithm”, Discovery (The International Daily journal),Vol. 29(107), Pages 22-28,March 2015.

[8] P. Nithyanandam, T. Ravichandran, N. M.Santron, E. Priyadarshini, “A Spatial Domain Image Steganography Technique Based on Matrix Embedding and Huffman Encoding”, International Journal of Computer Science and Security (IJCSS), Vol. 5, Issue No. 5, 2011.

[9] C.P.Sumathi, T.Santanam and G.Umamaheswari,” A Study of Various Steganographic Techniques Used for Information Hiding”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

[10] Ross J. Anderson, Fabien A. P. Petitcolas, “On the Limits of Steganography”, IEEE Journal on Selected Areas in Communications, Vol. 16, Issue No. 4, Pages No. 474 – 481, May, 1998.

[11] Dr. P V Ramaraju ,G.Nagaraju, M.Veeramanikanta, V.Sree Lekha, Mubashirunnisa, Y.Manojkumar , “Hiding and Encrypting Binary Images Using A Different Approach”, International Journal of Recent trends in Engineering and research, (IJRTER), Vol. 02, Issue No. 4 ,Pages 341-348,April 2016.

[12] Nicholas Hopper, Luis von Ahn, John Langford, “Provably Secure Steganography”, IEEE Transactions on Computers, Vol. 58, Issue No. 5, Pages No. 662 – 676, May, 2009.

[13] G. Nagaraju,Dr. P V Ramaraju,P. Ramakrishna,” Image Encryption After Hiding (IEAH) Technique For Color Images”, International IEEE Xplore digital library (Scopus), June 2016.

[14] Vaishali P , Pradyumna Bhat,” Transform Domain Techniques for Image Steganography”, International Journal Of Innovative Research In Electrical, Electronics, Instrumentation And Control Engineering, Vol. 3 , Special Issue. 1, April 2015

[15] Aryfandy Febryan , Tito Waluyo Purboyo and Randy Erfa Saputra3,” Steganography Methods on Text, Audio, Image and Video: A Survey”, International Journal of Applied Engineering Research

ISSN 0973-4562 Volume 12, Number 21 (2017) pp. 10485-10490.

[16] Dr.Ekta Walia, Payal Jainb, Navdeep, “An Analysis of LSB & DCT based Steganography”, Global Journal of Computer Science and Technology, Vol. 10, Issue No. 1, April, 2010.

[17] G. Naga Raju , Dr. P.V.Rama raju, P.Sai Priyanka,M. Mohan Krishna, M.S.V.Sravya, N.Hema Sai Kumar,” Steganography With LSB Binary Addition”, International Journal of Emerging Technologies and Innovative Research (JETIR) ,Vol. 4, Issue No. 11,Pages 138-142, November 2017.

[18] Neha Rani , Jyoti Chaudhary,”Text Steganography Techniques: A Review”, International Journal of Engineering Trends and Technology (IJETT) , Volume 4 Issue 7, july 2013.

[19] Ankit Chaudhary, J. Vasavada, J. L. Raheja, S. Kumar, M. Sharma, “A Hash based Approach for Secure Keyless Steganography in Lossless RGB Images”, 22nd International Conference on Computer Graphics and Vision, 2012

[20] Rubby Garg, Dr.Vijay Laxmi,“Various audio Steganography techniques for audio signals”, International Journal Of Engineering And Computer Science ISSN, Volume 5 Issue 10 Oct. 2016, Page No. 18682-18693

[21] Kushil Saini and Disha,” A Review On Video Steganography Techniques In Spatial Domain”,Recent Developments in Control ,Automation and Power Engineering,IEEE explore, May 2018.

[22] Shrikant S. Khaire, Dr. Sanjay L. Nalbalwar,” Steganography – Bit Plane Complexity Segmentation (BPCS) Technique”, International Journal Of Engineering Science And Technology ,Vol. 2(9), 2010,Pages 4860-4868.

[23] Alaa A.Jabbar Altaay,Shahrin Bin Sahib,Mazdak Zamani,” An Introduction to Image Steganography Techniques”**,**International Conference On Advanced Computer Science Applications And Technologies,Nov 2012.

[24] Chandra.M.Kota, Cherif Aissi, “Implementation of the RSA algorithm and its cryptanalysis”, ASEE Gulf-Southwest Annual Conference, American Society for Engineering Education, USA, 2002