# A step toward cryptography having high avalanche effect and PSNR with low cover file size and execution time

Archana Parihar[#1], Prof. Amit Saxena[*2]

[#] *M.Tech in computer technology and Application, Truba Institute of Engineering and Information technology Bhopal Madhya Pradesh India*

**Abstract** —*Data hiding is now a very potential area of research. Cryptography is a technique that states how you safe your information; it gives surety that your information is only shared with the person who is authenticated for the same. Steganography is a method that helps exchange confidential information such that nobody else can detect the existence of confidential message in any file /image. In almost numerous steganography algorithms, the authors would add a confidential message inmost a cover file without any encryption. But these types of steganography procedures are not secure to the extent that anyone can pull off the confidential message from the cover file. To provide better security, steganography method is used in combination with a cryptographic algorithm so that, even if anyone discovers the existence of confidential information, it is still impossible to understand. This work proposed a new encryption/decryption algorithm/technique and after encrypting the confidential message a new Steganography algorithm is applied to hide that secret message named HAEAPA( High Avalanche effect and PSNR algorithm . This combination provides better security for hiding confidential message and formerly reduces time complexity.*

**Keywords:**-*Security, Steganography, Encryption, Decryption, Cryptography.*

## INTRODUCTION

With the ever evolving internet technologies, digital media can be transmitted quickly and easily via the internet. However, the transmission of messages across internet still has to face various security problems. Therefore, protection of these secret messages for the period of transmission becomes a vital issue. This is where cryptography comes into the frame.

Cryptography is a technique to shuffle information using a confidential key in such a way that nobody can understand the original meaning of message without knowing the key get used to recover the original message. It is comes from the words 'kryptos' and 'graphein'.

**Encryption**: The procedure of conversion of original data (plain text) by converting it into an inconceivable form for understanding of data (cipher text) is called encryption. Encryption techniques are sometimes termed as code breaking.

As the exposure of internet increases day by day for the transfer or exchange of data, the requirement of better data security systems goes up proportionately. Various techniques to encrypt data have been in use. However, only the use of encryption methods are not sufficient enough to safeguard the confidential data contained by a cover file such as military information or any other confidential data, and hence the thought of more proficient data hiding comes in. In data hiding, the data is placed in a file called, host file and this host file size is bigger than the size of message file, and we wish to hide. For this reason, the term steganography gains light.

Steganography is a Greek word used for covered writing and it basically means "to hide in plain sight". The ability of discreetly hiding data inside any other data is steganography. The concept of steganography is used with combination of cryptography to provide high level of security. It is based on media type used to hide the text.

.

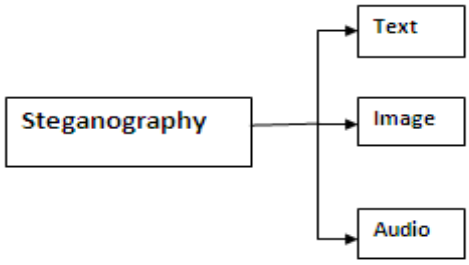



**Figure 1.1: Steganography Types**

***Text Steganography***: It hides the text behind some other text file. In this type of steganography the quantity of redundant text to hide the confidential message is limited in text files. Examples of text steganography techniques are selstive hiding, web pages etc.

***Image steganography***: this is the very difficult and famous techniques of steganography because of the limitation of HVS (Human visual System). The color vast range cannot be detected by eyes of

human and any irrelevant modification in the image quality than results from steganography is easily detected.

***Audio Steganography***: It is also one more hard form of steganography as humans are effortlessly capable of detecting even a minute modification in audio quality.

Steganography can also be separated into two types; (i) fragile (ii) robust .

**1. *Fragile***

Fragile steganography comprises implanting information within another file which may be damaged if any change in a information file predicted. Although this process is unbefitting for reproduction the copyright holder of the file, since it could be so effortlessly removed, but it is helpful in conditions where it is necessary to reveal that the file has not been altered. This steganography technique is easy to implement than robust methods.

**2. *Robust***

Robust marking goal are to implant information in this manner keen on a file so that it cannot be damaged easily. Although no mark is truly imperishable, a system could be measured as strong if the quantity of changes required to eliminate the mark will cause the file be rendered useless. For that reason the mark is secreted into that part of the file where its removal would be effortlessly perceived.

The other section of paper is arranged as follows. Section II shows the survey of literature on existing Steganography methods. The Section III shows the proposed work. The Section IV presented the results of experimental. The conclusion and future scope of the paper is shown in Section V.

## LITERATURE SURVEY

Many existing researchers have proposed various methods to embed the information message after encryption. Some researchers hide message contained by any document or text file or even sound file whereas others use image files.

Now-a-days everyone works on steganography systems to cover their objects using images. I have examined numerous such algorithms and lots of techniques that have been projected to conceal the secret data at the back of cover image without leaving any sort of mark.

Shashikala Channalli et al.(2009) had proposed technique of steganography for information hiding online on the instrument output screens. This method is utilized to announce a information message on a public area such as electronic advertising board in the region of sports stadium, a railway station or an airport. This technique of steganography is very analogous to the image and video steganography. For hiding secrete information authors had used Private marking system with steganography, LSB technique with symmetric key [1].

Fadhil Salman et al (2010) had used an idea cover a text file in an image file in such a manner that preclude, as much as possible, any suspicion of hidden text. For this authors had used the combine feature of steganography techniques and cryptography techniques. The proposed system uses DCT Quantization through steganography process. Authors apply two security levels: the RSA algorithm and the digital signature. Finally the image is stored in a JPEG format. Their proposed system called as asymmetric key Steganography [2].

Nath, Asoke et.al. (2010) had presented the work in which sound file is embedded within an image file , text file, word file , excel file , pdf file etc. The only limitation is that the size of cover file must be bigger as a minimum 10times to 20 times than the file in which it is embedded. Authors used three things to insert information message within the cover file (i) changing LSB, (ii) changing LSB+1 bit, (iii) changing LSB+3 bit. They have also introduced the password for obtaining the secret file. If the password is incorrect then nobody other than authorized person will be able to pull out message from the file.

Nath, Joyshree, and Asoke Nath(2011) had presented the work in which they have invented a new technique to hide encrypted confidential message within a cover file. Different method are used by authors to encrypting [4] and hiding a confidential message [3] .Authors have customized a new method called play fair to encrypt and decrypt to a new area named MSA method. The method named randomized key matrix using randomization is used for cryptography means for encryption of plain text file and for decryption of cipher text [4].

Das, Debanjan (2011) authors have desgined a new method called an integrated symmetric key cryptographic (DJMNA), a combination of two methods: (i) MGVC: Modified Generalized Vernam Cipher (ii) An extension of MSA method: DJSA. The algorithm Generalized Vernam Cipher can be expands text encryption to any kind of data encryption by applying ASCII code of all characters (0-255) [5].

Abed, Fadhil Salman (2012) Author have invented a new technique to cover confidential message in which two techniques were used (i)To encode information RSA cryptosystem is applied (ii) To hide the cipher information proposed fractal image compression method is applied. [6].

Niemiec, Marcin, and Lukasz Machowski(2012) In this work authors have presented an algorithm named symmetric cryptographic with S boxes . During encryption process new S-box technique were used. These S boxes were key dependent and ensure high level confidentiality. The S-box method is depends on the Rijndael S-box and currently it is used in the AES algorithm on the other side, the

method is as general as and it may be based on any S-box. [7].

Mathur, Akanksha(2012) presented an algorithm in which data encryption and decryption is based on ASCII value of that data. For data encryption/ decryption, secret key is modifying by adding another string. It is basically a kind of symmetric encryption algorithm. For encryption/ decryption same key with some modification is used. This algorithm operates when the input length and the length of key are same [8].

Dey, Somdip(2012) have presented a new cryptographic technique, called SD-AREE,this technique is used to eliminate repetitive terms comes in a message, at the time of encryption , so that it becomes unattainable for a anyone to pullout or calculate the actual information from the encrypted message. SD-AREE technique comes from the slighter change in two techniques named (i) modified Caesar Cipher Technique (ii) advanced bit-manipulation cryptographic method. This method removes all the repetitive words from the encrypted file [9].

Rishav , Jeeyan , Debanjan (2012) had designed a new process for hiding any encrypted confidential message. Authors have invented the thought of hiding message within any file (text/ASCII /DOC), by changing the blank/white space characters etc. of a file. The confidential message is initially encrypted and hided using Modified Generalized Vernam Cipher Method (MGVCM)and inside any ASCII file respectively .In this paper authors have tried to change the cover file by inserting each and every bit of confidential message file into a eight randomly selected blank space [10].

Xing Tang et. al. (2013) presented a promising algorithm to conceal an information in Word document, which by converting the RGB values of character and underline. Meanwhile, authors have designed and implemented a text information hiding system that is based on RGB algorithm. The structure, mechanism and process of the system is described in detail. The comparisons of experimental results state that the algorithm has outstanding performance in visual. Furthermore, the system also expands the hidden capacity and improves the imperceptibility of carrier document [11].

Juneja, Mamta et.al. (2013) have designed a unique technique for information security. In this work authors presented steganography method in which confidential message bit is embedded in LSB of nonadjacent random pixel locations in edges of images. 1-3-4 LSBs of red, blue green, components of arbitrarily selected pixels across flat areas. No original cover image is required for the pulling out of the confidential message. The prime goal of this work is to propose a solution that is robust, effective and to make it very hard for human eye to predict and detect the subsistence of any secret data contained by the host image. The proposed solution has not only achieved what was required but has also increased the data hiding capacity of the key image by utilizing all the pixels [12].

Devi, Kshetrimayum et.al. (2013) had proposed a technique that is rely on image steganography .this technique was a combination of LSB techniques and technique named pseudo random encoding and used to advance the security of the communication of images. In the LSB approach, the cover image LSB bits to be secreted without deteriorating the actual quality of the cover image significantly. In Pseudo-Random technique a generator called Pseudo-Random Number uses random-key as a seed during embedding process. Both the techniques uses a stego-key when message is embedding within the cover image .This stego-key reduce the chance of receiving attack by the attacker [13].

Paul, Manas, et.al.(2013) proposed a technique based on symmetric key cryptographic on session bit level .and this methods is known as Spiral Matrix Based Bit Orientation Technique (SMBBOT). SMBBOT deem the binary bit stream as a input plain text. This binary stream is separated into convenient sized blocks with variable lengths stream for the duration of encryption. These blocks bits are received from MSB to LSB .Finally they have to fit into a matrix(square matrix).This square matrix breaks into 2x2 sub-matrices. Column-wise Bits are collected from all 2x2 sub-matrices . From this encrypted binary stream then cipher text is generated. The cipher text is measured as binary bit string for decryption process. Decrypted binary string is formed after taking the bits from the square matrix and then the reverse concept of Spiral Matrix is followed. The binary form of decrypted stream is used to regenerate plain text [14].

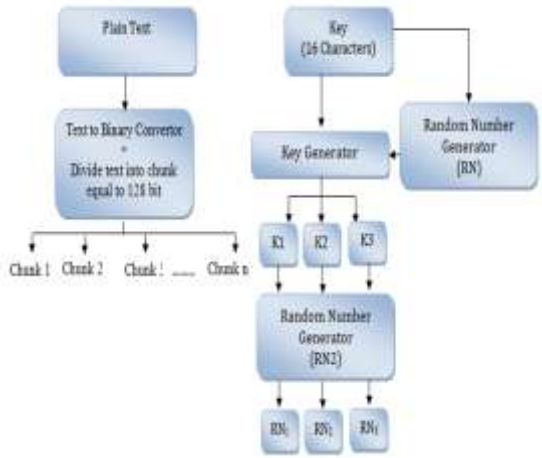
## Proposed work

In most of the research work, the authors have been tried to implant some secret message within any cover file in an encrypted form so that no one will be able to pull out the actual confidential message. Here I combined steganography method with a cryptographic encryption/decryption algorithm named High Avalanche effect and PSNR algorithm (HAEAPA) so that even if anyone discovers the subsistence of secret information, it is still not understandable. This method provides high security and better performance.

### *3.1 Encryption algorithm:*

1. Input plain text and key of size 128bits.
2. Generate random number($R_N$) with the help of key by using following steps:
   a) Sum ASCII value of all characters and store it in sum.
   b) Perform Mod operation on sum by 128.
   c) Result of step b is $R_N$.

3. Generate three different keys ($k_1$,$k_2$ & $k_3$)with the help of original key using following steps:
   a) Convert the original key into binary format i.e. key1=$k_1$.
   b) Perform XOR operation on every bit of $k_1$ with its $R_N$ position bit and store the result in $k_1$.
   c) Next perform circular left rotation on $k_1$ by $R_N$.
   d) Repeat steps b& c on $k_1$ to get $k_2$.
   e) $k_1$, $k_2$, $k_3$ are the generated new keys.
4. Convert the text into binary format
5. Perform padding operation to make it multiple of 128 bit.
6. Next divide the plain text into number of chunks , where each chunk is of size 128 bits
7. Repeat the following step for each chunks:
8. Perform XOR operation on each bits of chunk with its respective $R_N$ position bit & store the result in $P_T$.
   a) Perform XOR operation of PT with $k_1$and store the result in $P_1$.
   b) Generate a random number $R_{N2}$ by using key $k_1$ by calculating number of 1's in key $k_1$.
   c) Perform XOR operation on each bit of PT with its respective RN1 position bit & store the result in $P_T$.
   d) Repeat the steps a,b,c,d with $k_2$ on $P_T$.
   e) Again repeat steps a,b,c,d with $k_3$ on the result of step e.
9. Final result of chunk is the Cipher text of respective chunk.



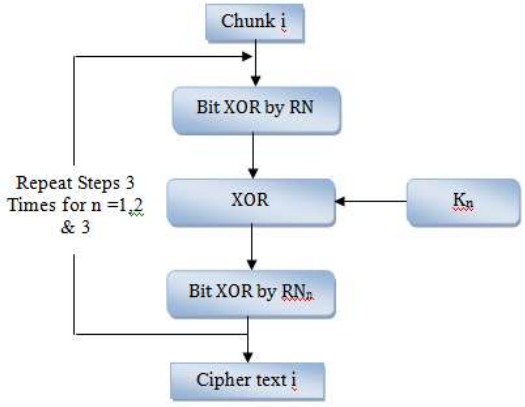




**Figure 3.1: Block Diagram of Proposed HAEAP encryption Algorithm**

***3.2 Decryption algorithm*:** it's just a reverse process of encryption algorithm

***3.3 Steganography algorithm:***

Step1: the Cipher text Converted into binary format.

Step2: If binary string number of 1's is more than number of 0's than invert all the bits of string.

Step3: Hide the string behind every character of MS word file written in black colour by using LSB method.

## Experimental Results

Here, I experimentally evaluated Proposed HAEAP algorithm and compare it with RJDA Algorithm and Information hiding system based on RGB algorithm.

### *4.1 Evaluation method and experimental result of proposed HAEAP algorithm*

Encryption plays an important part in information security. Therefore, it is necessary to evaluate the performance of encryption and decryption algorithms. The evaluation is done on two parameters: execution time and avalanche effect. I analyzed and compare the **HAEAP algorithm with RJDA [10]** on both above parameters and compare proposed HAEAP algorithm with RJDA and information hiding system based RGB algorithm with only on PSNR. In this section, I showed the experimental results of **HAEAP algorithm**

#### *4.1.1Execution time of proposed HAEAP Encryption and decryption Algorithm*

Execution time of encryption algorithm is the time required to encrypt the file and that of the decryption algorithm is the time required to decrypt the file. Execution time increases with the increase in file size.

**Table 4.1: Execution time of proposed HAEAP encryption Algorithm and RJDA encryption Algorithm**

| File Size in KB | Encryption Algorithm ( Execution Time in Second) | |
|---|---|---|
| | RJDA [2012] | Proposed HAEAP Algorithm |
| **1 KB** | 9.362 | 0.040 |
| **5 KB** | 16.985 | 0.050 |
| **10 KB** | 25.145 | 0.090 |

It is clear from the table 4.1 & figure 4.1 that the execution time of HAEAP algorithm is very less as compare to RJDA algorithm. Example 1KB file require 9.362 second to encrypt where as Proposed HAEAP algorithm require 0.040 seconds.

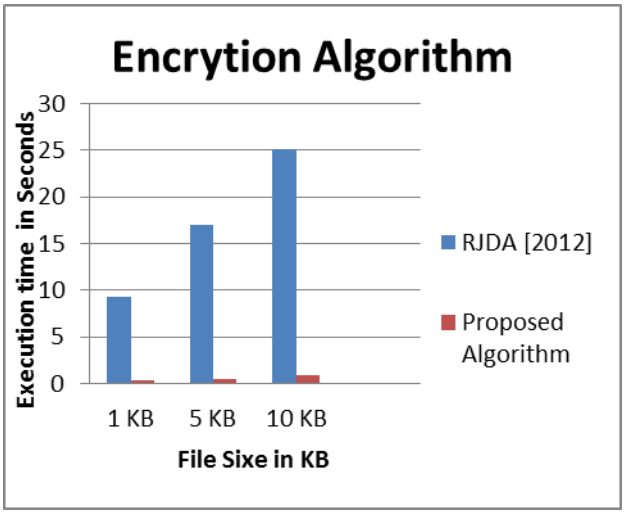



Figure 4.1: Results of Execution time of proposed HAEAP encryption algorithm and RJDA algorithm (2012)

Table 4.2: Results of execution time of RJDA Decryption algorithm

It is clear from the table 4.2 & figure 4.2 that the proposed HAEAP algorithm execution time of is very low as compare to RJDA algorithm. Example 1KB file require 9.358 second to decrypt where as HAEAP algorithm require 0.040 seconds.

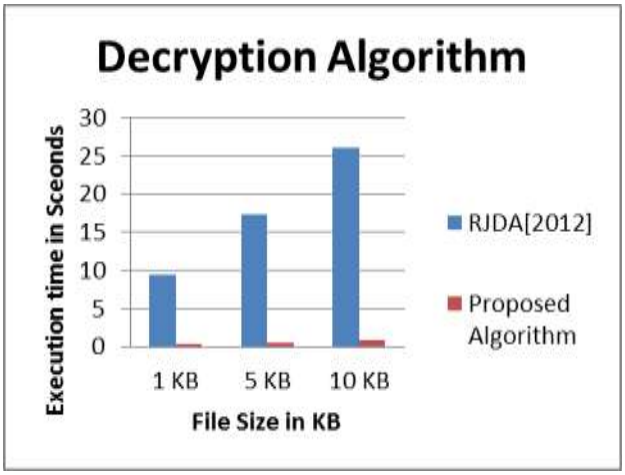



**Figure 4.2: Results of Execution time of HAEAP decryption algorithm and RJDA (2012).**

***4.1.2 Avalanche effect***

It is an enviable property in which if you change a one bit in input then its lead to a major bit change in output of cipher text. Some cipher systems have the property in which a small change in the input results in a very large change in the output.

**Table 4.3: Avalanche effect of RJDA algorithm & HAEAP algorithm**

| File Size in KB | Avalanche Effect | |
|---|---|---|
| | RJDA[2012] | Proposed HAEAP Algorithm |
| **Single bit change in key** | 43.15% | 51.2% |

It is clear from the table 4.3 that the avalanche effect of HAEAP algorithm is greater than the RJDA algorithm [2012].

***4.1.3 Peak Signal to Noise Ratio***

Peak signal to noise ratio is a term used to find ratio between the highest possible value of a input signal and the rate of distorting noise that change the quality of its representation. PSNR is generally articulated in concerned of decibel.

**Table 4.4: PSNR Comparison between proposed HAEAP algorithm, information hiding based on RGB algorithm (2013) and RJDA algorithm (2012).**

| File Size in KB | PSNR Value | | |
|---|---|---|---|
| | information hiding based on RGB algorithm [2013] | RJDA [2012] | Proposed HAEAP Algorithm |
| 1 KB | 66.89 | 20.63 | 72.54 |

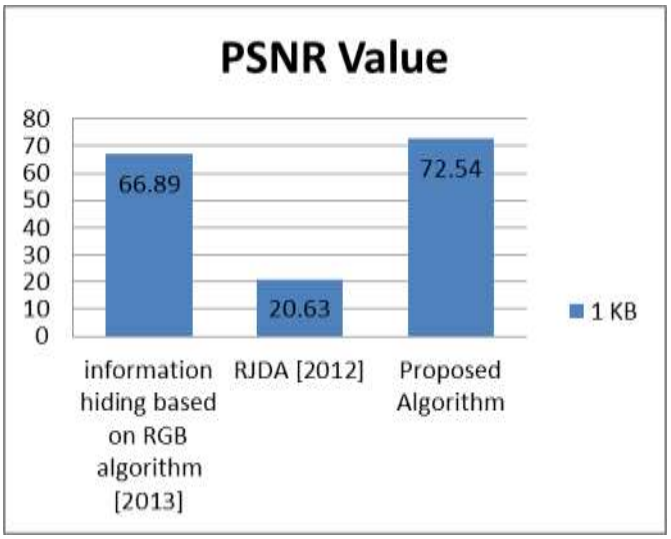



***Figure 4.5PSNR Comparison between Information hiding based on RGB (2013), RJDA Algorithm (2012) and Proposed HAEAP algorithm.***

Table 4.4 shows the experimental results and figure 4.5 shows that Peak to Signal ratio of proposed HAEAP algorithm is for 1 KB file is higher as compared to that of Information hiding based on RGB algorithm and RJDA Algorithm.

## CONCLUSION

With the bullet like evolution of technologies in computer and internet, data security is an important concern in today's life. In this paper, I have studied lots of cryptographic algorithms and proposed an improved algorithm and analyzed it with two of them naming RJDA and information hiding based RGB algorithm. Steganography has been known and practiced for centuries. Previously, people would use manual methods for data hiding in which data is placed inside some host file or an object. But after the arrival of digital steganography, the entire method of data hiding has been modified. Digital steganography has totally overtaken the old traditional methods in recent world of computers and internet. Also with the arrival of new methods, the attackers have invented newer techniques to break the code. This in turn gives rise to invention of more secure methods which are even more complex. This paper aims o develop an algorithm which provides more security to the confidential data by first encrypt it by applying a new secure encryption algorithm and then hiding it in some text or document files abundant on the internet and not providing any sort of loophole to penetrate for the attacker. Improvisations on this work would be possible in the future in a number of ways: Firstly, this security system encrypts and embeds a confidential message into which is essentially a text document. Now if this cipher message might be further encrypted and sent as a secret message, the attacker would not be able to retrieve the original message. Secondly, this method could also be improved to compress the original secret message file and then encrypt more than one small compressed secret message files and embed them randomly.

## References


1) Thorsten Holz Frederic Raynal, "Detecting Honeypots and other suspicious environments," in Proceedings of IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY 2005.

2) Abed, Fadhil Salman, and Nada Abdul Aziz Mustafa. "A Proposed Technique for Information Hiding Based on DCT." Int. J. Adv. Comp. Techn. 2.5 (2010): 140-152

3) Nath, Asoke, Sankar Das, and Amlan Chakrabarti. "Data Hiding and Retrieval." Computational Intelligence and Communication Networks (CICN), 2010 International Conference on. IEEE, 2010.

4) Nath, Joyshree, and Asoke Nath. "Advanced Steganography Algorithm using encrypted secret message." International journal of advanced computer science and applications 2.3 (2011)

5) Das, Debanjan, et al. "An integrated symmetric key cryptography algorithm using Generalised Modified Vernam Cipher method and DJSA method: DJMNA symmetric key algorithm." Information and Communication Technologies (WICT), 2011 World Congress on. IEEE, 2011.

6) Abed, Fadhil Salman. "A Proposed Encoding and Hiding Text in an Image by using Fractal Image Compression." International Journal on Computer Science and Engineering (IJCSE) 4.01 (2012): 1-13.

7) Niemiec, Marcin, and Lukasz Machowski. "A new symmetric block cipher based on key-dependent S-boxes." Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2012 4th International Congress on. IEEE, 2012.

8) Mathur, Akanksha. "A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms." International Journal on Computer Science and Engineering (IJCSE) 4.9 (2012): 1650-1657.

9) Dey, Somdip. "SD-AREE: An Advanced Modified Caesar Cipher Method to Exclude Repetition from a Message." International Journal of Information and Network Security (IJINS) 1.2 (2012): 67-76.

10) Ray, Rishav, et al. "A new Challenge of hiding any encrypted secret message inside any Text/ASCII file or in MS word file: RJDA Algorithm." Communication Systems and Network Technologies (CSNT), 2012 International Conference on. IEEE, 2012.

11) Tang, Xing, and Mingsong Chen. "Design and implementation of information hiding system based on RGB." Consumer Electronics, Communications and Networks (CECNet), 2013 3rd International Conference on. IEEE, 2013.

12) Juneja, Mamta, and Parvinder S. Sandhu. "An Improved LSB Based Steganography Technique for RGB Color Images." International Journal of Computer and Communication Engineering 2.4 (2013).

13) Devi, Kshetrimayum Jenita. A Sesure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique. Diss. National Institute of Technology-Rourkela, 2013.

14) Paul, Manas, and Jyotsna Kumar Mandal. "A Novel Symmetric Key Cryptographic Technique at Bit Level Based on Spiral Matrix Concept." arXiv preprint arXiv:1305.0807 (2013).

15) Pandey, Shriya, and Manish Shrivastava. "A Survey on Time Efficient and Secure Data Hiding Algorithm." International Journal of Emerging Technology and Advanced Engineering Volume 4, Issue 6, June, 2014.

16) Archana Parihar , Amit saxena "Survey on Digital Data Hiding using steganography" International Journal of Recents Trends in Engineering & Research Volume 3, Issue 3, March , 2017.