

Secured Transmission of Text using Double Encryption Algorithm

K. Kumaresan¹, Ashwin V², Divya Darshini R³, Jayasona G⁴

¹Assistant Professor, Department of Computer Science & Engineering, K.S.R. College of Engineering, Tiruchengode-637215, Tamilnadu, India. Email: mkkumz@gmail.com

^{2,3,4}Student, Department of Computer Science & Engineering, K.S.R. College of Engineering, Tiruchengode-637215, Tamilnadu, India. Email: ashwinkle58@gmail.com¹, ammudivya275@gmail.com², Jayasonajj@gmail.com³

Abstract - This paper discusses how a text file is to be kept secret while transmitting from sender to receiver. The paper is intended to present techniques for encryption and Steganography. Steganography is the practice of covering messages or information in host data or text or an image. Digital images are the most popular whose frequency of occurrence is more on internet. Steganography, which is a method for securing a message than cryptography that cache the content of the message and not the existence of message. Steganography, which is a tool which allows hidden transmission of information over the communication channel. Stego image are provided by combining the secret message with the carrier image. In this paper, double coding algorithms are intimate to hide the encrypted text in a host image which then makes the secret message not easy to detect without retrieval. This paper presents a technique that could transmit with a high security.

Keywords - Cryptography, Lower bit insertion, Private key, Pseudo Noise, Public key, Steganography.

I. INTRODUCTION

Due to the rise of internet the most important factor of communication and information technology is information security. Cryptography is the technique of securing the secrecy of communicating. Many methods have been developed for encryption and decryption of data in order to maintain the secrecy of messages [1]. Sometimes it is not enough to just maintain the secrecy of a message, also necessary to keep the existence of the message secret. The technique is used to implement Steganography [2]. Steganography is distant from cryptography. The goal of cryptography is to keep the message secret whereas the goal of steganography is to keep the existence of message secret. Both the techniques provide ways to protect the information from unwanted parties but neither technology alone is perfect [3]. If any presence of hidden information is revealed or suspected, the purpose of steganography is then defeated. The strength of steganography can be augmented by combining with cryptography [4], [5]. In this paper, two different encryption techniques are used to encrypt the message: RSA and DES encryption techniques. This paper is intended to present further information about these algorithms and steganography technique. Basically, cryptography is divided into two types: symmetric encryption and asymmetric encryption.

Symmetric encryption is the earliest and the best-known technique. A secret key can have number, or a string of random letters, tests messages to change the content. As there is no significant time delay for encryption and decryption, implementation of symmetric cryptography can be highly effective. Symmetric cryptography authenticates as the data encrypted with one symmetric key cannot be decrypted with another symmetric key. Therefore, the symmetric key is secured by the two parties to encrypt messages, they can communicate with each other until the decrypted message make sense. The popular algorithms for symmetric encryption are DES, AES, IDEA, Blowfish, Triple DES, Two fish, Serpent [6]. Asymmetric Encryption is nothing but the Public Key Cryptography. In this encryption, there is a pair of keys. Where one key can encrypt which is called public key and the other key can decrypt and hence it is called private key. Protocols such as OpenPGP SSH depend upon asymmetric encryption and various digital functions. In this type of encryption public key can be replaced and changed by a third party. When it is changed the data can easily be decrypted by the third party. It is necessary to verify whether the correct public key of person has been transmitted or not. The popular algorithms for asymmetric encryption are RSA, DSA, El Gamal, ECC [7]. Steganography covers the information within computer files. In Digital Steganography, communication of message is possible through image, video, text, audio or in protocol of transport layer. Media files are optimal for steganographic transmission because of the larger sizes [8], [9]. Steganography depends on the type of media being used to hide the messages, normally include text, images, audio files and network protocols utilized in network transmissions. The cover file indicates the kind of steganography. In linguistic steganography, the data is hidden in the font, style etc. In technical steganography, the cover files are used. In text steganography, the line spacing or spacing between words is changed to make the data hidden in the text file stored. In this technique, varying a very small amount of spacing is not differentiable to the human eye [10]. In audio steganography, the noise behind the original audio or the echo of audio as noise is used to hide a secret message. Filters

and amplifiers can be used to amplify the noise to find the message [8], [11]. In image steganography, the pixel values are changed based on the message such that it cannot be noticed by the human eye. In video steganography, as the video is a combination of image and audio both image and audio steganographic techniques can be applied [11]. In image steganography, the cover file is an image. Images have various file formats such as JPEG, BMP, PNG, etc. In these image formats, BMP file has more size as it is an uncompressed image and JPEG file format uses lossy compression whereas PNG uses lossless compression techniques. Hence for bit replacement techniques jpg format is not suitable as some data can be lost. Hence it is necessary to go with BMP or PNG image formats. Both the image formats are 24-bit images where 8 bits are reserved for each pixel of red, green and blue planes. By different combinations of these colours in 8 bits, each can obtain 16 million colour shades. Image steganography can be further classified into two types based on domain: Frequency domain technique and spatial domain technique.

Transformation or frequency domain techniques are based on manipulating the transform coefficients of an image instead of the pixels in an image itself. These techniques are suited to process the image in consistent with the frequency content. The orthogonal transform of the image consists of two components magnitude and phase. The magnitude contains the frequency content of the image. The phase helps to restore the image back to the spatial domain. Generally, transform domain allows operation on the frequency content of the image, and thus high- frequency content like edges and other refined information will simply be intensified. DWT is the tool used for image decomposition. It's helpful for processing of non-stationary signals. DWT is predicated on small waves that are known as wavelets of varied frequency and amplitude. Wavelet transform provides both frequency and contiguous description of an image. It shows an image as a summation of sinusoids of varying frequencies and magnitudes [12].

Table I: The % Color Change Based on a Change in Bit Position.

| BIT POSITION | % CHANGE IN COLOUR |
|--------------|--------------------|
| 1 | 0.39% |
| 2 | 0.78% |
| 3 | 1.57% |
| 4 | 3.13% |
| 5 | 6.27% |
| 6 | 12.55% |
| 7 | 25.01% |
| 8 | 50.1% |

Spatial domain techniques are based on manipulating the pixel values of the image according to the secret message. In LSB insertion method the pixel values and their LSB positions are manipulated such that the LSB position gives the hidden message [13]. From Table I, it has been understood said that inserting the encrypted data into the lower bits of host media does not vary the color whereas inserting in the higher bits varies the color. Hence it is preferable to insert data in the lower bits of an image. In these techniques, JPEG cannot be used as some data is lost due to compression [14]. In pixel differentiator technique, the difference in the least two significant bits stores the data. Based on the message, the LSB position is changed so that XOR of least two significant bits stores the data [15].

II. CRYPTOGRAPHY

A. RSA encryption

RSA is the first practical asymmetric key encryption technique. RSA is the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, designed the algorithm . So different men tried to break the code and failed hence it can be said that the technique is secure. In RSA algorithm the message is always taken in the form of ASCII values. In this algorithm two large prime numbers, p and q are taken. n is the product of p and q. Select p and q in such a way that the ASCII values of message taken are lies between 0 to n-1. Then $g = (p-1)*(q-1)$ and e are premeditated such that the greatest common divisor of g and e is 1. And also get d value such that $(g*e) \bmod g$ is 1. Now (e, n) is said to be public key while (d, n) is said to be a private key. Whenever there is a communication between Alice and Bob. Bob gives his public key publicly. Cheryl also knows the public key when Alice encrypts the data using the public key and transmits it to Bob. Though Cheryl knows the public key he cannot decrypt the data without knowing the private key. Only Bob can decrypt the data as he has the private key. So, RSA algorithm has a secured transmission. To encrypt the data, cipher being the encrypted text and message being the secret message. $\text{cipher} = (\text{message } e) \bmod n$. $\text{plain} = (\text{cipher } d) \bmod n$ [7]. Similarly, while decrypting, the received cipher text is decrypted to get back the pain text. As large values of p and q are taken, practically in digital devices, the remainder is zero. By applying the rules of Vedic mathematics and Modular arithmetic, data can be encrypted [16]. Using this algorithm the number of bytes of data remains same, but only the text is encrypted.

DES Encryption

The Data encryption standard (DES) was developed by IBM and adopted as national customary in 1977 [6]. It is first encryption algorithm approved by U.S. Government for Public, which ensured that the algorithm was quickly adopted by industries where the encryption necessity is high [17]. DES is a block cipher which means the encryption in terms of blocks. As the length of key increases, it is difficult for the third party to guess the key and hence takes more time to perform more operations [18]. The 64-bit key is taken and is reduced to 56 bit for various other operations. Pseudo-Noise is generated using the linear feedback shift registers in this paper [19]. 5 shift registers which are connected to each other and the output of one register gets added to the PN sequence [20]. Whenever there is a change in the initial value of the shift registers there will be a change in 64-bit key. Using permutations 56 bits are selected from 64-bit key and rearranged. Fifty-Six bits are divided into two halves, 16 bits from each half, form an initial key. Now each half is shifted circularly to find the second key similarly as mentioned above. Similarly, 16 different keys are found for 16 different iterations. DES is a 64block cipher, only 64 bits are encrypted at a time. Hence divide the message into blocks such that it contains 64 bits each, if necessary, zeros are appended in the last. Now take each block and divide it into two halves say L1 and R1. By using the two rules the encryption can be done for $i=2$ to 15.

$$L(i) = R(i-1)$$

$$R(i) = L(i) + f(R(i-1),k(i))$$

where addition indicates modulo 2 addition, k indicates the different 32-bit keys and f indicates the set of functions that can be applied. Now R16L16 combined together gives the encrypted text. The same process is applied in reverse way for decryption [6]. This produces strong avalanche effect. Whenever there is a change in a single bit in the message there will be large variation in the encrypted text, this is called avalanche effect.

III. PROPOSED METHOD

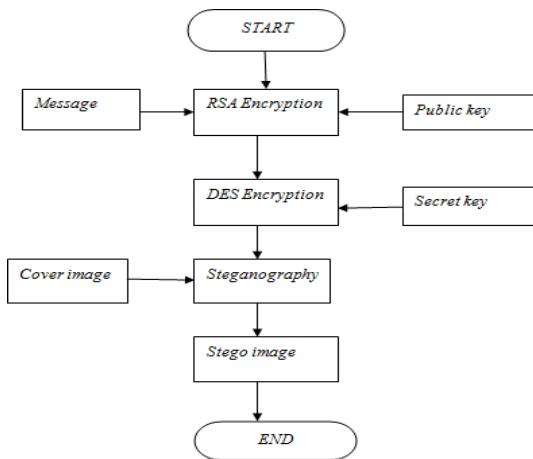


Fig 1: Transmitter Side

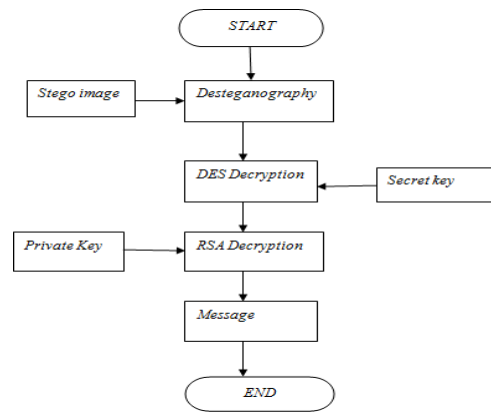


Fig 2: Receiver Side

This paper presents a methodology to obtain high security. In this technique, both cryptography and steganography are combined with each other to obtain high security. In Cryptography, two types of techniques are used, one from symmetric technique and other from asymmetric encryption. In symmetric encryption, DES algorithm and RSA algorithm in asymmetric encryption are used. In this method, initially the selected message is encrypted using RSA algorithm with the public key. This encrypted text is further encrypted using DES algorithm. As DES algorithm has only one key which is a secret key, it is generated using linear feedback shift registers [3]. In this encrypted text, another byte of data is added to indicate the initial value of shift registers. Another byte of data is added to indicate the length of the encrypted text or message which is being stored in the image. Pixel values are selected in randomly in such a way that they are multiples of 3. To store a long message, more number of pixels are needed. Hence instead of storing a bit of data in each color, in this method the first three least significant bits of data is stored in first three least significant bits of selected pixels in red plane. Similarly the following three least significant bits of data is stored in first three least significant bits of selected pixels in green plane. The two most significant bits of data is stored in first two least significant bits of selected pixels in blue plane. So that on byte of data in each pixel. Storing one byte in each pixel helps to store the longer message. For a good PSNR value, select the image which has more number of pixels that is large size image. Selecting large image reduces the mean square error which increases the Peak Signal to Noise Ratio [18]. Using this method, the message can be transmitted with higher PSNR.

To retrieve the data from the image, the pixel values are obtained from the image in which the data is stored. Then in the first pixel as the total text size is stored, discover the pixel values till text size is reached. Thus the first byte indicates the initial value of shift registers for generation of PN Sequence. After generation of PN sequence, using the already intended 64-bit key and apply DES decryption process with the 16 sets of keys generated from PN sequence. The obtained result is decrypted by applying RSA decryption process with the private key. As Private Key is only known to

you, only you can get the decrypted value. After decryption, the decrypted text size and original message are verified to ensure that there should not be any error during transmission and reception.

IV. RESULTS





The message taken to transmit through above process is:

"Hi!

Good Morning."

For the message taken above the ASCII values are 72, 105, 33, 13, 10, 71, 111, 111, 100, 32, 77, 111, 144, 110, 105, 110, 103 46. The length of the message is 18 bytes. RSA Encryption is applied, taking the public key as (3,145). The length of RSA Encrypted text will be same 18 bytes. The length of text in DES is multiple of 8. The obtained result is further encrypted using DES algorithm by taking the initial value of shift registers as [1 1 0 0]. As zeroes are appended to RSA encrypted text, the length will be 24 bytes by appending 6 zeros. The initial byte of data stored in the image is 25, which represents the length of message stored. Next byte stored in image is 56, which is the modified value of shift register. Modified value of shift register is the decimal converted value of shift register and then randomly selected value is added to acquire more security, in this case it is chosen as 32. Then the DES encrypted text is stored in an image which has 61200 pixels. But in this method as discussed above the message is stored in pixels of 3 planes where pixels are selected at integral multiples of 3. Using this, PSNR and MSE calculated for images of different universities and colleges. Similarly, to decrypt, the private key to be used is [75,145]. After the process of decryption, it has been observed that both the transmitted and received messages are same. Hence, the message is said to be transmitted successfully. This message after being transmitted successfully, at the receiver side operation starts. At the receiver side, the message is recovered from the lower bits of pixels in an image. This message being in encrypted form will be decrypted using Private Key and secret key. These keys will help to decrypt the data and will give the original message. For DES decryption, secret key will be used. For RSA decryption, the private key is used. MSE and PSNR values for various images are tabulated as shown in Table II. MSE is the mean square error which can be calculated host image and stego image. Whenever the data is stored in the image, the corresponding pixel values changes and this change in pixel values is an error. PSNR is the Peak Signal to Noise Ratio which is calculated from the obtained MSE values for different images. The MSE and PSNR values are same whenever the algorithm is tested for different formats of same image and same encrypted message. So, it has been observed that the performance metrics MSE and PSNR are independent of the format used.

Table II: The MSE and PSNR Values Calculated for Logos of Different Colleges and Universities for a Text Message of Length 18 Bytes.

| IMAGE | Mean Square Error | Peak Signal to Noise ratio |
|-------------------------------------------------------------------------------------|-------------------|----------------------------|
|  | 0.0040 | 72.1703 |
|  | 0.0046 | 71.5277 |
|  | 0.0042 | 71.9305 |
|  | 0.0046 | 71.5193 |

| | | |
|-------------------------------------------------------------------------------------|--------|---------|
|  | 0.0028 | 73.6893 |
|  | 0.0046 | 71.5300 |
|  | 0.0028 | 73.6638 |
|  | 0.0046 | 71.5287 |
|  | 0.0046 | 71.5247 |
|  | 0.0024 | 74.4426 |
|  | 0.0046 | 71.5287 |

Another taken to through process is:

message transmit above

"There is a spy in the department.
The autopsy report and blood reports are manipulated.
Also, the details regarding the raid are sent."

The ASCII values for the messages are 84, 104, 101, 32, 112, 101, 114, 115, 111,110, 110, 32, 121,105, 110, 103, 32, 102, 111, 114, 32, 105, 115, 32,110, 111, 116, 32, 116, 104, 101, 32, 109, 117, 114,100, 101, 114, 101, 114, 33, 13. 10, 84, 104, 101, 114, 101, 32, 105, 115, 32, 97, 32, 115, 121, 32, 105, 110,32, 116, 104, 101, 32, 100, 101, 112, 97, 114, 116,109, 101, 110, 116, 46, 13, 10, 84, 104, 101, 32, 97,117, 116, 111, 112, 115, 121, 32, 114, 101, 112, 111,114, 116, 32, 97, 110, 100, 32, 98, 108, 111, 111, 100,32, 114, 101, 112, 111, 114, 116, 115, 32, 104, 97,115, 32, 98, 101, 101, 110, 32, 97, 110, 105, 112, 117,108, 97, 116, 101, 100, 46, 13, 10, 65, 108, 115, 111,32, 116, 104, 101, 32, 100, 101, 116, 97, 105, 108,115, 32, 114, 101, 103, 97, 114, 100, 105, 110, 103,32, 116, 104, 101, 32, 114, 97, 105, 100, 32, 104, 97,115, 32, 98, 101, 101,110.

The length of the message is 198 bytes. For a better understanding of the paper, the length of the message is increased and size of the image is decreased. Applying RSA Encryption taking the public key as (3,253). The length of RSA Encrypted text will be same 198 bytes. The length of text in DES is multiple of 8. To the obtained result applying DES encryption with the initial value of shift registers being changed to [1 0 0 1 1]. As zeroes are appended to RSA encrypted text the length will be 200 bytes by appending 2 zeros. The initial byte of data stored in the image is 201, which represents the length of message stored. Next byte stored in image is 51, which is the modified value of shift register. Modified value of shift register is the decimal converted value of shift register and then randomly selected value is added to acquire more security, in this case it is chosen as 32. Then the DES encrypted text is stored in an image which has 26100 pixels. But in this method as discussed above the message is stored in pixels of 3 planes where pixels are selected at integral multiples of 3. Using, PSNR and MSE calculated for different images of various universities and colleges. Similarly, to decrypt the private key to be used is [147,253]. After the process of decryption it has been observed that both the transmitted and received messages are same. Hence, the message is said to be transmitted successfully. The

obtained MSE and PSNR values for various images are shown in Table III. MSE is mean of square of the difference in original image and stego image.

Preferable format for this technique is PNG format because lossless compression is done, hence occupies less memory and PNG format is more frequently used on the internet. As JPEG is lossy compression there is a chance of losing the data, so it is not recommended.

Table III: The MSE and PSNR Values Calculated for Logos of Different Colleges and Universities for a Text Message of Length 198 Bytes.

| IMAGE | Mean Square Error | Peak Signal to Noise ratio |
|-------------------------------------------------------------------------------------|-------------------|----------------------------|
|  | 0.0699 | 59.7186 |
|  | 0.0928 | 58.4891 |
|  | 0.0882 | 58.7080 |
|  | 0.0916 | 58.5455 |
|  | 0.0576 | 60.5615 |
|  | 0.0849 | 58.8760 |
|  | 0.0594 | 60.4255 |
|  | 0.0805 | 59.1081 |
|  | 0.0909 | 58.5760 |
|  | 0.0531 | 60.9158 |
|  | 0.0764 | 59.3360 |

V. CONCLUSION

This paper ensure that using the double encryption techniques, the data is highly secured such that the third party cannot read the content of the text without decrypting for which the third party need to know the 64 bit key value. That

means he needs to know the circuit connections of feedback shift registers and the initial value of shift registers. To know the 64-bit key, it is necessary to know the initial value and the combination of shift registers. Still it cannot be sure, as few bits are removed from the 64-bit key, further shifted circularly and then few selected bits are used to generate the each set of the key with 32 bits each. So it is difficult to break the DES encrypted text. Similarly, in RSA algorithm, it is required to know the private key to decrypt the data with the present algorithm it takes around 56 to 72 hours to find the private key from the public key. Whenever larger prime numbers are taken the time taken to obtain private key from the public key is more. In RSA, private key can be recognized from the public key. It is must to find the prime factors which can be p and q, from which the private key can be created. As prime number values keep increasing, the factorization gets difficult. Hence it is recommended to take large prime numbers to encrypt the text using RSA algorithm. Using steganography makes sure that data is stored in an image without much change in the color of an image. These techniques independently are turning insecure with advancement in technology. Hence these techniques are changed or modernized so that it makes the text secure. From the Table II and Table III, it has been observed that as the message length increases, then the error increases. Hence as the capacity increases, error increases which in turn decreases the PSNR. And it is observed that the quality of stego images are good and security is high.

REFERENCES

- [1] Ekwe A.O, Okonba B.J, "Cryptography: A Useful and Widely Used Tool in Today's Engineering Security", International Journal of Engineering Trends and Technology, Volume 12, No.4, pp.196-198, June 2014.
- [2] T.Morkel, J.H.P Eloff, M.S. Oliver, "An overview of image steganography", Information and Computer security Architecture Research group, Annual Information Security South Africa Conference, July 2005.
- [3] Arvind kumar, KM. Pooja, "Steganography- A data Hiding Technique," International Journal of Computer Applications, Volume 9, No.7, pp.19-23, November 2010.
- [4] Y. Manjula, K.B.Shivakumar, "Enhanced Secure Image Steganography using Double Encryption Algorithms," International Conference on Computing for Sustainable Global Development, IEEE 2016, pp.705-708.
- [5] Xinyi Zhou, Wei Gong, Wen Long Fu, Lian Jing Jin, "An Improved Method for LSB Based Color Image Steganography combined with Cryptography", International Conference on Computer and Information Science, IEEE, pp.1-4, 2016.
- [6] D. Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks", IBM J.RES. Develop. Volume 38 No. 3, May 1994, pp.243-250
- [7] A. Shamir, R.L. Rivest, L. Adleman, "A method for Obtaining Digital Signatures and Public key Cryptosystems," Communications of the ACM, pp.120-126, 1978.
- [8] Navneet Kaur, Sunny Behal, "A survey on various types of Steganography and Analysis of Hiding Techniques," International Journal of Engineering Trends and Technology, Volume 11, No. 8, pp. 388-392, May 2014.
- [9] Neha Rani, Jyothi Chaudhary, "Text Steganography: A Review", International Journal of Engineering Trends and Technology, vol. 4, no. 7, pp.3013-3015, July 2013.
- [10] Beenish Mehboob, Rashid Aziz Faruqi, "A Steganography Implementation", International Symposium on Biometrics and Security Technologies, IEEE, pp.1-5, 2008.
- [11] Shaveta Mahajan, Arpindersingh, "A Review of Methods and Approach for Secure Steganography", Indian Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, pp. 67-70, October 2012.
- [12] Sudhanshi Sharma, Umesh Kumar, "Review of Transform Domain Techniques for Image Steganography", International Journal of Science and Research, Volume 4, Issue 5, pp.194-197, May 2015.
- [13] Wang. H, Wang. S, "Cyber warfare: Steganography vs Steganalysis", Communications of ACM, -Volume 47 No.10, October 2004, pp.76-82.
- [14] V.Lokeswara Reddy, Dr.A.Subramanyam, Dr.P.Chenna Reddy, "Implementation of LSB steganography and its evaluation for various file formats", International Journal of Advanced Networking Applications, Volume 2, Issue 5, pp.868-872, April 2011.
- [15] Kamaldeep Joshi, Pooja Dhankar, Rajkumar Yadav, "A New Image Steganography Method in Spatial Domain using XOR", Annual IEEE India Conference, IEEE, pp.1-6, 2015.
- [16] Sri Devi, Manajai D.H, "Modular Arithmetic in RSA cryptography," International Journal Of Advanced Computer research, Volume4, No. 4, Issue-17, pp-973- 978, December-2014.
- [17] Sung-Jo Han, Heang-Soo Oh, Jongan Park, "The improved Data Encryption Standard (DES) Algorithm", Department of Electronic Engineering, Chousan University, South Korea. IEEE, pp.1310-1314, 1996.
- [18] Ali Mir Arif Mir Asif, Shaikh Abdul Hannan, "A Review on Classical and Modern Encryption Techniques", International Journal of Engineering Trends and Technology, Volume 12, No.4, pp. 199-203, June 2014.
- [19] Afaq Ahmad, Sayyid Samir Al-Bursaidi, Mufeed Juma Al- Musharafi, " On Properties of PN Sequences generated by LFSR- a Generalized study and Simulation Modeling", Indian Journal of Science and Technology, Volume 6, Issue 10, pp.5351-5358, October 2013.
- [20] Rupendra kumar Pathak, Shweta Meena, "LSB Based Image Steganography Using PN Sequence & GCD Transform", International Conference on Computational Intelligence and Computer Research, IEEE, pp.1-5, 2015.