A Survey on CryptoSteganography: A Multilayer Security Data Hiding

Bhushan S. Bafna[1], Bhagyashree H. Mutha[2], Avinash D. Gawali [3], Ankush J. Govind [4]

[1,2,3,4] Student, Department of Computer Engineering,
SRES COE, Kopargaon, Savitribai Phule, Pune University
Maharashtra, India

ABSTRACT

Now a days there is a challenges faced by Data or Information Security Field. We have to make this data free from harm during transmission. The primary aim is to make an application which enables sensible information by covering securely in statistically undetectable communication channel. The two important concepts of securely transmitting information or data over a medium like internet are Steganography and Cryptography. Steganography is the art of secure communication which aims to hide the secret or sensitive information into a cover medium while observing the least possible statistical detectability. Cryptography is a scheme which decodes secret messages into several encrypted forms and distributes them. These both are used to assure security. But none of them can simply satisfy the basic needs of security i.e. the properties such as robustness, undetectability and capacity etc.

*A new technique based on the merging of both Cryptography and Steganography which can be named as "**Cryptosteganography**" is necessary which overcomes each other's limitations and make hard for the intruders to attack or steal sensitive information is being proposed. To provide again more security to this new technology of Cryptosteganography a newest methodology is added to it which can be named as "**Multilayer Steganography**". This new technique makes use of two cover files to strongly hiding of the Crypto-Stego file for providing very strong security in transmission of important data. The problem of the size of file during transmission is also resolved by "**Multilayer Cryptosteganography Compression**". Application of this extends the horizon of data and file embedding and secrecy of data. Thus the scope is better than the existing Cryptography and Steganography systems which only the operations of data hiding and message embedding in the file.*

Keyword: - *Encyption, Decryption, CryptoSteganography, A multilayered Steganography, Multilayer Cryptosteganography Compression-Decompression.*

1. INTRODUCTION

The speedy evolution of data transfer through internet has made it simpler to send the data exact and quicker to the destination. To transfer the data to destination there are many transmission media like e-mails, social sites etc. At the same time it is may be easier to modify and misuse the valuable information through hacking. So, in order to transfer the sensitive data securely to the destination excluding any alteration, there are many methodologies like Cryptography and Steganography. One of the reasons why the attackers become successful in intrusion is that they have an opportunity to read and comprehend most of the information from the system. Intruders may reveal the information to others, misuse or modify the information, misrepresent them to an individual/ organization or use them to plan even some more severe attacks. One of the solutions to this problem is through the use of steganography and cryptography. But among them some methods are implemented to break these approach security. So there is need to
make the communication more secure among the existing one.

1.1 Cryptography

Cryptography encodes information in such way that nobody can read it, except the person who holds the key. Cryptography comes from Greek word where "Crypto" means "Secret" and "Graphy" means "Writing"[5]. As shown in Figure 1.1 the cryptography provides the security to the data file.The Sender sends the data in plain text which is readable manner then using one of encryption algorithm the plain text converts into cipher text which is in unreadable form.

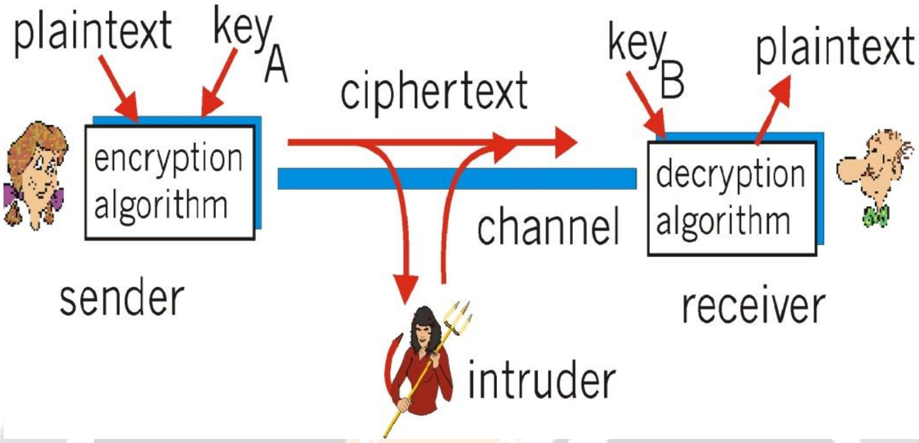


Figure 1.1: Working of Cryptography

So intruders cant see the actual data.When the plain text reached to the receiver, at receiver side the decryption algorithm used to converting cipher text back to plain text and actual data is observed at receiver side. This whole process of cryptography is performed be the "key" which decided by both for the purpose of encryption and decryption.

1.2 Existing Steganography

Steganography is not truly a method of encrypting message but hiding them within something else to enable them to pass unobserved. The word steganography comes from Greek word where "Steganos" means "Covered" and "Graphy" means "Writing"[5]. The various forms of data in steganography can be audio, video, text, images etc. The basic model of Steganography consists of three components:

- The Carrier image: The carrier image is also called the cover object that will carry the message that is to be hidden.
- The Message: A message can be anything like data, file or image etc.
- The Key: A key is used to decode/decipher/discover the hidden message.

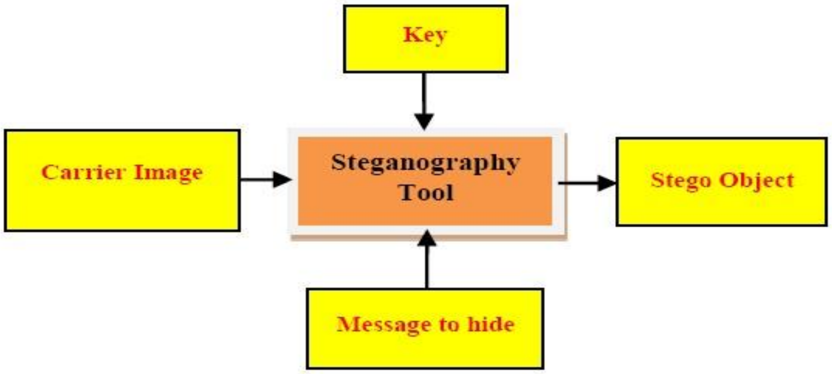


Figure 1.2: Working of Steganography

As shown in Figure 1.2, The Steganography just put a one carrier image or cover file among the encrypted data so the real file is hide among the medium which hides real file form attacker.

1.3 New Advance Steganography

Cover file + Message to be hidden -----> Stego file .... (Secure)
Now,
Master file + Stego file -------> Advance Stego file .... (More Secure)
The Master cover file is again applied on cover file under which already encrypted data is embedded.So in this way Advance Steganography is increases more privacy and secure data transmission.

1.4 CryptoSteganography

Merging of Cryptography and new advance Steganography wich can be named as "Cryptosteganography".

1.5 Multilayer Cryptosteganography Compression

Multilayer Cryptosteganography Compression is the art of reducing the number of bits needed to store or transmit data. Compression can be either lossless(text or programs) or lossy(image,audio,video)[13].

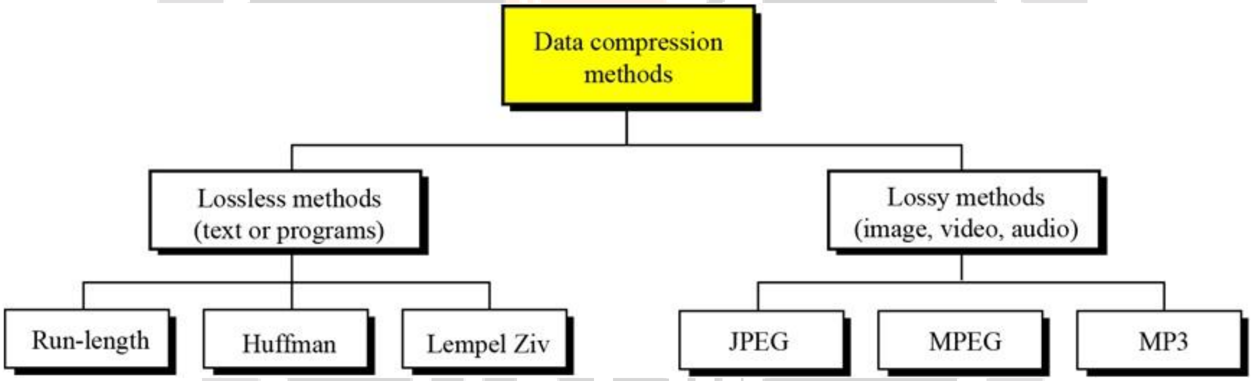

Data compression methods
Lossless methods (text or programs)
Lossy methods (image, video, audio)
Run-length
Huffman
Lempel Ziv
JPEG
MPEG
MP3

Figure 1.3: Data Compression Methods

There are different Data Compression Methods as shown in above Figure 1.3.

2. LITERATURE SURVEY

In this section we discuss the different Methodologies Review/ Literature Review and Motivation Outcomes from it.

2.1 Review of Methodologies

The 32-bit RISC processor block can be used to different cryptography algorithms execution, The real time data security has been built for a data storage device [1].

Steganography investigation made for stego-images, bearing a secret data are statistically natural. The change happen to it is consistently biased in a given way [2].

Steganography writing on a wet paper and recognize it using a simple variable-rate random linear code which devotes the sender a commodious flexibility and control management over the process of embedding and thus it is practically suitable for implementation [3].
WiMAX (Worldwide Interoperability for Microwave Access) technology to security, vulnerabilities and risks analysis [4].

Construction and implementation of new stego based algorithm based on hiding the max amount of data file into color BMP image [5].

Text steganography using SMS-texting language; a new method for secure communication [6].

Packet-oriented telemetry data encapsulation with number of compression stream algorithms that can be decoded, rendered and also observed by any type of standard PDF viewer [7].

Idea about implementation of stego-analysis system by highlighting the weak point, disadvantages, stages of attack of steganography [8].

Encrypt and decrypt the data audio-video sequences using optical crypto technology which is based on double random phase encoding algorithm [9].

Merging of cryptography and steganography to overcome of each other's limitations and weaknesses [10].

Improvement in MSE, PSNR, and MSE value by the analysis of existing stegoanalysis methods, by this researchers can improve secure steganography techniques [11].

VSS (Visual secret sharing) is a visual cryptography method that perform decoding of secret messages in several enlarged shares, and distributes it into various participants [12].

Hiding data in scrambled images with a new approach- double layer security data hiding in which data hiding perform significant attention with alternate way to ensure security [13].

Design of multiple levels for steganography technology with LSB at the time of data transmission based on architectural design of data security with multilevel stego system [14].

2.2 Motivational Outcomes

The different outcomes are motivated for the current system by reviewing the methodologies explained in Section 2.1 as follows:

- There is very big chances of hacking the secret message so for assurance of data security it need to provide Cryptography to convert the readable data into unreadable form.
- There is also fewer chances of breaking Steganography by sego-analysis but for more assurance of data security it need to design a new multi-layered Steganography.
- The already existed problem of data size obviously increased by this multi-layering techniques so to solve it need to design data compression technique for the system.

3. SYSTEM OVERVIEW

The system has a architectural overview which are discussed in following section.

- The Basic Crypto-Stego-Encoder and Crypto-Stego-Decoder Architecture:

This is the section where encoding performs at sender side and decoding performs at destination side. Crypto-Stego-encoder as in Figure 3.1 collects user information such as the message file, cover file and the secret key to be used for the message encryption and perform the necessary action depending on the user requirement. The encoder encrypt the message file content using the key provided, then may compress the file before encoding the message under the original image using the key supplied to form stego-image and then send it via the communication medium to the destination.

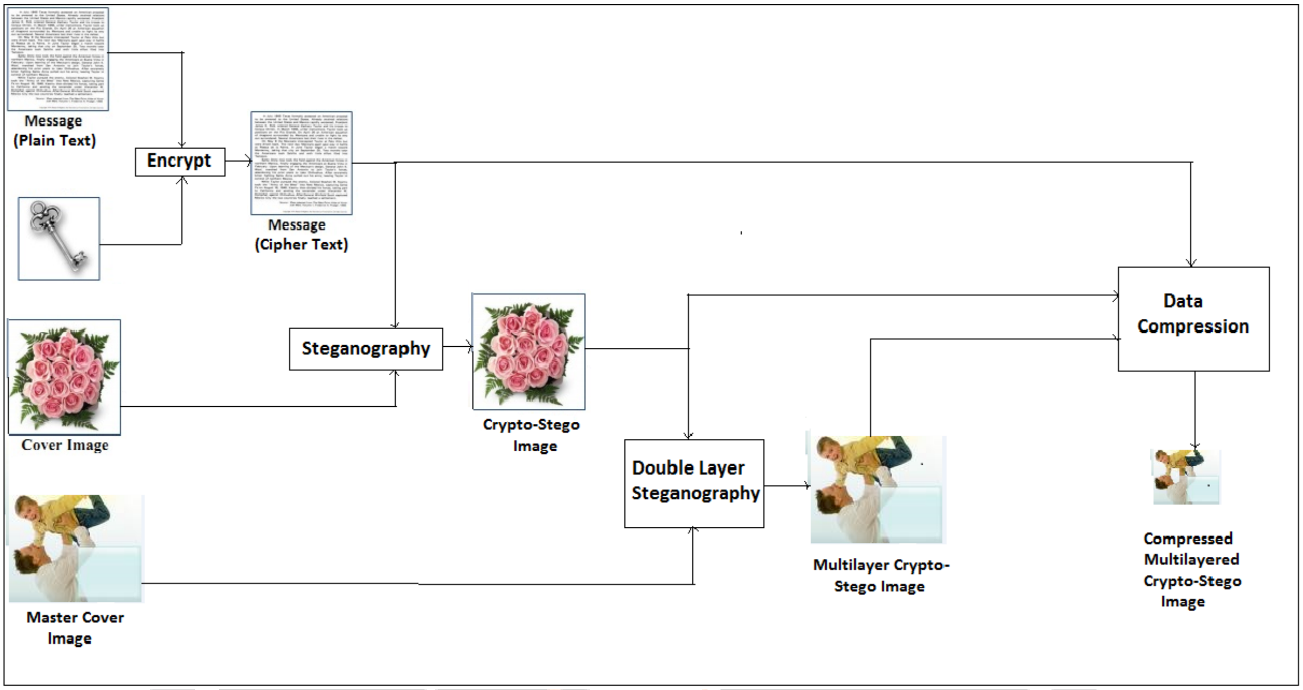


Figure 3.1: The Working of a Multilayer CryptoSteganography Data Hiding Encoder Architecture

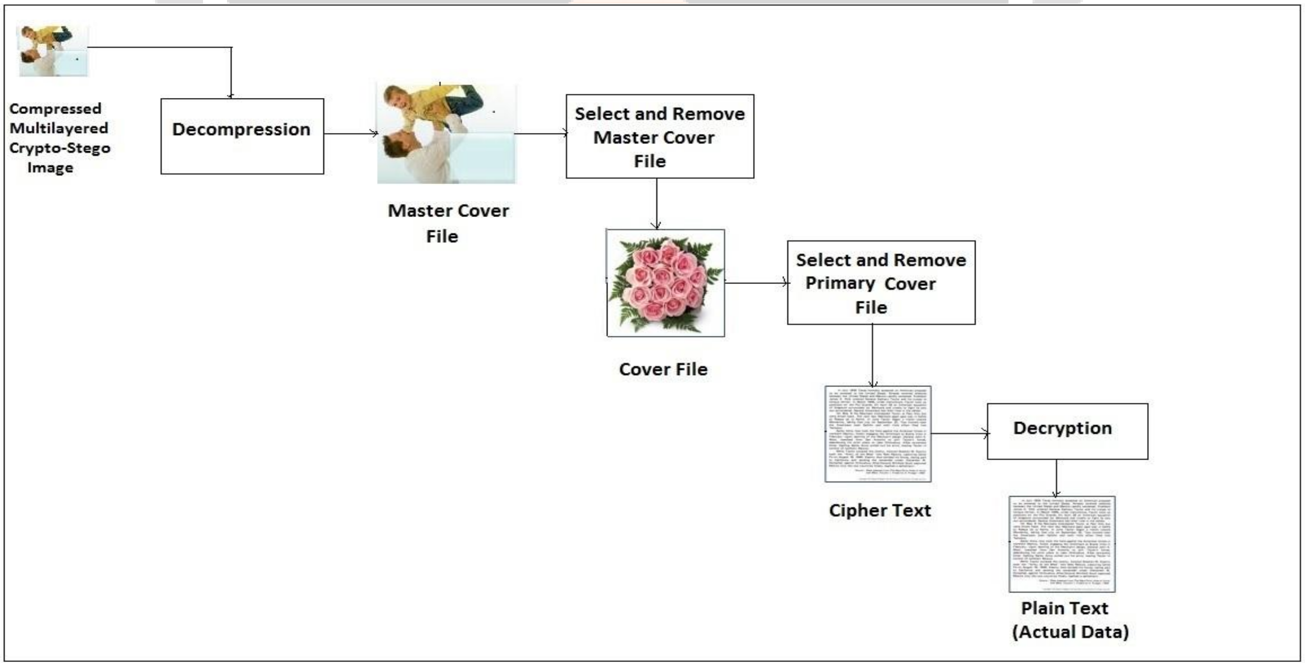


Figure 3.2: The Working of a Multilayer CryptoSteganography Data Hiding Decoder Architecture

- **DES (Data Encryption Standard) Algorithm:**

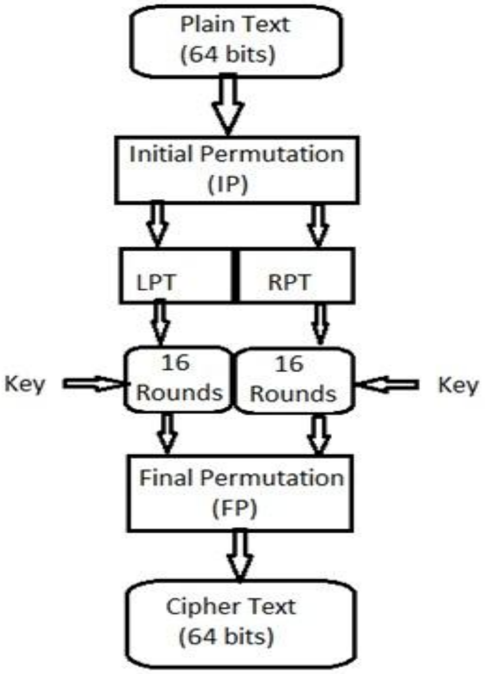


Figure 3.3: DES Algorithmic Steps

1) plain text (64-bit) block is handed over to an Initial Permutation (IP) function.
2) Initial Permutation is performed on plain text.
3) IP produces two halves of permuted block.

- Left Plain Text (LPT) and
- Right Palin Text (RPT)

4) 16 rounds of process of encryption performed by each LPT and RPT goes through, each with its own key.
5) At the end LPT and RPT are both rejoined and on the combined block the Final Permutation (FP) is performed
6) The result is 64 bit cipher text, as shown in Figure 3.3.

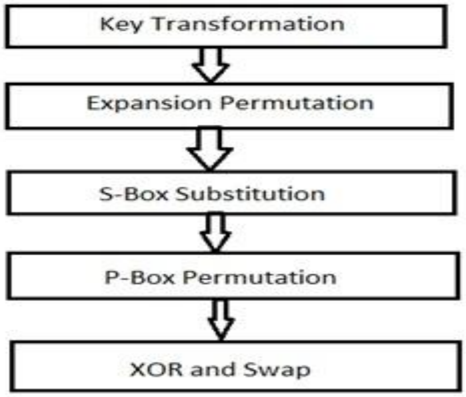
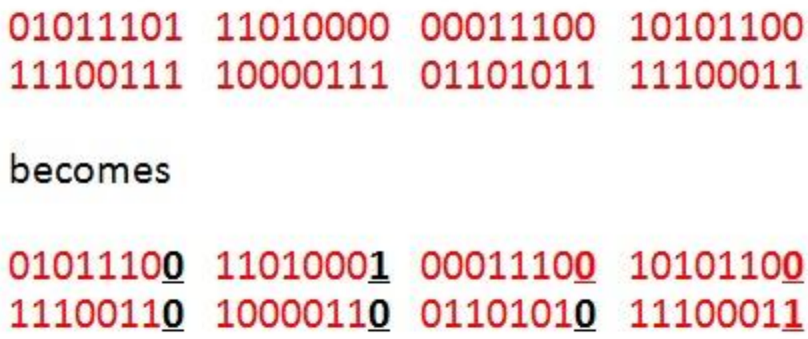


Figure 3.4: Rounds in DES

- ➢ Initial Permutation (IP) happen only once.IP replaces the first bit of original plain text block with 58th bit of original plain text block,second bit with the 50th bit and so on.
- ➢ After IP is done,the resulting 64 bit text block is divided into two half block,each with 32 bits.(LPT and RPT)
- ➢ Now 16 Rounds are performed on these two blocks.
- ➢ Each 16 Rounds are consists of following broad level steps as shown in Figure 3.4.

- **LSB (Least Significant Bit) Algorithm:**

- ➢ The most common and simplest method of steganography is LSB (least significant bit).To encode the hidden information the ones bit of a byte is used.
- ➢ Suppose in the following 8 bytes of a carrier file we want to encode the letter A (ASCII 65 or binary 01000001)



01011101 11010000 00011100 10101100
11100111 10000111 01101011 11100011

becomes

0101110**0** 1101000**1** 0001110**0** 1010110**0**
1110011**0** 1000011**0** 0110101**0** 1110001**1**

4. CONCLUSION

A new high capacity and highly secure data hiding has been presented. The master cover file is most essential for providing more data security as multi-layer Steganography including Cryptography provide a wide range of data security. The system produces a good quality stego images for a fairly high amount of payload with compression based system. The double layer security coupled with high capacity and good perceptual transparency make the proposed system a very good candidate system for convert communications.

ACKNOWLEDGEMENT

We want to thank our guide Prof. S. N. Gunjal for his continued support but for the motivation and fruitful advises in accomplishing this task.

REFERENCES

[1] HoWon Kim, Member, IEEE, and Sunggu Lee, Member, IEEE*, "Design and Implementation of a Private and Public Key Crypto Processor and Application to a Security System"*, In IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, FEBRUARY 2004 pp. 214 - 224.
[2] Alvaro Martn, Guillermo Sapiro, and Gadiel Seroussi, Fellow, IEEE., *"Is Image Steganography Natural?, In IEEE Transaction On Image Processing"*, VOL. 14, NO. 12, DECEMBER 2005, pp. 2040 - 2050.
[3] Jessica Fridrich, Miroslav Goljan, Petr Lisonek, and David Soukal, *"Writing on Wet Paper, In IEEE Transactions On Signal Processing"*, VOL. 53, NO. 10, OCTOBER 2005, pp.3923 - 3935.
[4] Jamshed Hasan, *"Security Issues of IEEE 802.16 (WiMAX)"*, Originally published in the Proceedings of 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5th December, 2006.
[5] Nameer N. EL-Emam, "*Hiding a Large Amount of Data with High Security Using Steganography Algorithm."*, Journal of Computer Science 3 (4): 223-232, 2007 ISSN 1549-3636, pp.223 - 232.
[6] Shirali-Shahreza, M.H. ; Dept. of Comput. Eng., Yazd Univ., Yazd ; Shirali- Shahreza, M., *"Text Steganography in chat"*, Internet, 2007. ICI 2007. 3rd IEEE/IFIP 47 International Conference in Central Asia on , pp.1 - 5.
[7] Intell. Syst. Div., NASA AmesMaluf, D.A. Res. Center, Moffett Field, CA ; Tran, P.B. ; Tran, D., *"Effective Data Representation and Compression in Ground Data Systems"*, In Aerospace Conference, 2008 IEEE ,pp. 1 - 7.
[8] Naji, A.W. Dept. of Electr. and Comput. Eng., Int. Islamic Univ. Malaysia, Kuala Lumpur, Malaysia, Gunawan, T.S. , Hameed, S.A. , Zaidan, B.B. more authors , "*Stego- Analysis Chain, Session One Investigations on Steganography Weakness vs Stego- Analysis System for Multimedia File*", Computer Science and Information Technology - Spring Conference, 2009. IACSITSC 09., pp. 405 - 409.
[9] Guizani, S. ; Coll. of Eng., Alfaisal Univ., Riyadh, Saudi Arabia ; Nasser, N. , *"An audio/video crypto Adaptive optical steganography technique"*, In Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International , pp. 1057 - 1062.
[10] Md. Khalid Imam Rahmani, Kamiya Arora and Naina Pal, "*A Crypto-Steganography: A Survey"*, In IJACSA, Vol.5, No.7, 2014, pp. 149 - 155.
[11] Deepali V. Patil and Mr. Shatendra Dubey, *"Review Paper On Image Steganography"*, In International Journal of Research In Computer Aplications And Robotics Vol.2 Issue 6.June 2014, pp. 35 - 40.
[12] Cheng-Chi Lee, Hong-Hao Chen, Hung-Ting Liu, Guo-Wei Chen, and Chwei- Shyong Tsai , *"A new visual cryptography with multi-level encoding"*, In journal of visual languages and computing, Vol.25, 2014, pp. 243 - 250.
[13] Shabir A. Parah, Javaid A. Sheikh, Abdul M. Hafiz and G.M. Bhat, *"Data hiding in scrambled images : A new double layer security data hiding technique"* , In computers and electrical engineering , Vol.40, 2014, pp. 70 - 82.
[14] Adedayo Adeolu Adeniji, Micheal Esiefarienrhe, and Naison Gasale, *"Architectural Design of Multi Level Steganography System for Data Transmission"*, In Intl Conf. on Chemical Engineering and Advanced Computational Technologies (ICCEACT2014) Nov. 24-25, 2014 Pretoria (South Africa), pp. 78 - 83.

BIOGRAPHIES

Bafna Bhushan is pursuing B.E. Computer Engg. in SRES COE, Kopargaon. His area of research interests include Sensisitve Information or Data Security.

Bhagyashree Mutha is pursuing B.E. Computer Engg. in SRES COE, Kopargaon. Her area of research interests include Sensisitve Information or Data Security.

Gawali Avinash is pursuing B.E. Computer Engg. in SRES COE, Kopargaon. His area of research interests include Sensisitve Information or Data Security.

Govind Ankush is pursuing B.E. Computer Engg. in SRES COE, Kopargaon. His area of research interests include Sensisitve Information or Data Security.