Proposing a LSB Bit Plane steganography and Embedding (LBPSE) Model for Secure Messaging Using LSB Steganography with Encryption

Dr. Amit Kumar Chaturvedi [#1] & Jahangeer Mohi ud din Lone [*2]

*Asst. Prof., Engineering College, Ajmer[#1], Ph.D. Scholar, Mewar University, Chittorgarh[*2]*

*amit0581@gmail.com[#1], jahangeer.lone@gmail.com[*2]*

Abstract: *There are various communication techniques available in the world. Some provides the facility to do the communication in public or private mode. Every communication technique has some qualities and some drawbacks, but one thing is common that is the requirement of privacy and security of data from malfunctioning of the communication. During this covid-19 pandemic throughout the world everything is closed in their place and the importance and need of these communication techniques feels by everyone. There are two methods for secure communication: (i) Cryptography, and (ii) Steganography. Steganography is a technique in which communication contents either text, image, audio, or video file hided under a cover that may be an image, text, or video. Encryption is a technique that will secure the data by using encryption and decryption. In this paper we will present an idea of secure messaging using both encryption and steganography and proposes an innovative model LBPSE for secure messaging using LSB Steganography with encryption.*

Keywords: **LSB, Bit Plane, embedding, steganography, encryption, message hiding.**

1. INTRODUCTION

The need of secure messaging is not a new concept, from the ancient time to till date it is always a need for the professionals. Secure messaging not only needed for the administration or governance but also for personal data security. There are two methods for secure messaging: (1) Steganography, and (2) Cryptography. Steganography is an art used for secure messaging, in which the message is hided under a cover and this cover may be text, image, audio, or video. Cryptography is another technique for secure messaging, in which the message in converted into another form by using the encryption. In cryptography the one can clearly identify that there is something secret that due to this reason it is converted into another form. But in case of steganography, the cover will not be converted into any other form. It may be a plain text, image, etc. Only message will be hided under this cover.

Image steganography techniques can be categorized as: (1) Spatial Domain Methods, (2) Spread Spectrum Technique, (3) Statistical Technique, (4) Transform Domain Technique, (5) Distortion Technique, and (6) Masking and Filtering.

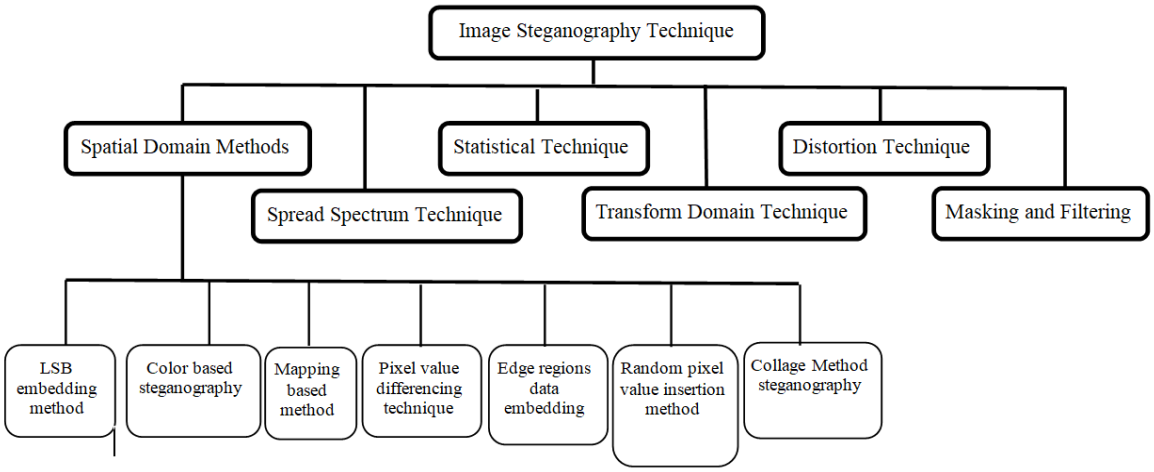

Figure 1: Image steganography techniques

LSB stands for Least Significant bit. The idea behind LSB embedding is that if we change the last bit value of a pixel, there won't be much visible change in the color. In this paper, we are using the bit plane of an image for hiding the message under a LSB bit plane cover image. The LSB bit plane under which message was hided, i.e. "Stego image", will be then embedded with the rest of the bit planes to again recombining the image.

This proposal is innovative because the use of encryption algorithm for encrypting the message as well as using the steganography with LSB bit plane in this proposal for providing better security for sending message using a shared communication environment, like cloud computing. Another important feature of this proposal is the use of encryption algorithm AES-128 or 256. AES encryption technique is very strong among other encryption algorithms in its category.

Steganalysis is the reverse process of steganography. Steganalysis is a process used for obtaining the hidden message under a cover. If the encryption algorithm is also used with steganography then the complexity for steganalysis also increases accordingly. So, the process of steaganalysis is complex here in this proposal and that definitely makes the message security more strong.

2. PROPOSED MODEL AND METHODOLOGY

In covid-19 pandemic, the only medium used by the common public, professionals, and business organization for communication is the internet, because of its availability anywhere, anytime, throughout the world. The intruders, cyber attackers, or spywares are also active to steal the useful information from the commonly shared medium of communication internet. So, the need of securing useful information using steganography like methods is increased more. The Least Significant Based steganography is a very useful method, because to do steganalysis and exaction of the message from the cover requires specialized software. If encryption method like AES-128 or AES-256 is also applied with the LSB steganography, it will provide very strong and secure method of communication over a share communication medium like internet.

Here, we are proposing a model called as "LSB bit plane steganography and embedding (LBPSE)" for secure message communication over a shared communication medium like public cloud. The model is illustrated below in the figure 2 and figure 3.

The figure 2 explain the process flow of the LSB bit plane steganography and embedding (LBPSE) model, which takes an image as input and then separating its all eight (08) bit planes of the selected grey scale image. Now, the Bit Plane 1 will be selected as the cover for hiding the secret message and it will be stored as an image file in the store. The next step is to take the message as input that is to be sent secretly as input file and then encrypting the message with a "secret key" using AES algorithm. The encrypted message is ready and the LSB Bit Plane is also separately stored. The next step is to hide the encrypted message under this LSB image cover and then the LBPSE model will generate the "stego image". This "stego image" is also an LSB image and basically it is the Bit Plane 1 that is one of the parts of the eight separated Bit Planes from the original image. The model in the next step will merge these all the Bit Planes, i.e. Bit Plane 1 or "Stego image" and the rest seven Bit Planes to recombine the original image. This recombined image is denoted as the "recombined image" in this model. This recombined image will have the encrypted message. So, this part of the image uses the concept of steganography with encryption algorithm and finally we get an "recombined stego image" containing the

secret message. This image is now ready to send over the shared communication medium and will safely carry the message to the receiver.

The figure 3 illustrates the process flow chart for the extraction of the secret message from the "stego image", i.e. "recombined image" received from the shared communication medium like cloud computing by the receiver. At the receiver end, the "recombined image" will be first selected as input file and then the LBPSE model will separate all the eight bit planes of this "recombined image" or "stego image". The first Bit Plane is the our target image and this part of the recombined image having the secret message. So, the LBPSE model separate this Bit Plane and store it separately. Then the process of steganalysis is applied on this Bit Plane 1 with the "secret key" used for encryption of the message. The message will be unhide successfully and stored at the specified location of the system.

So, the LSB bit plane steganography and embedding (LBPSE) model provides an innovative approach for sending secret messages on a shared communication medium like cloud computing.

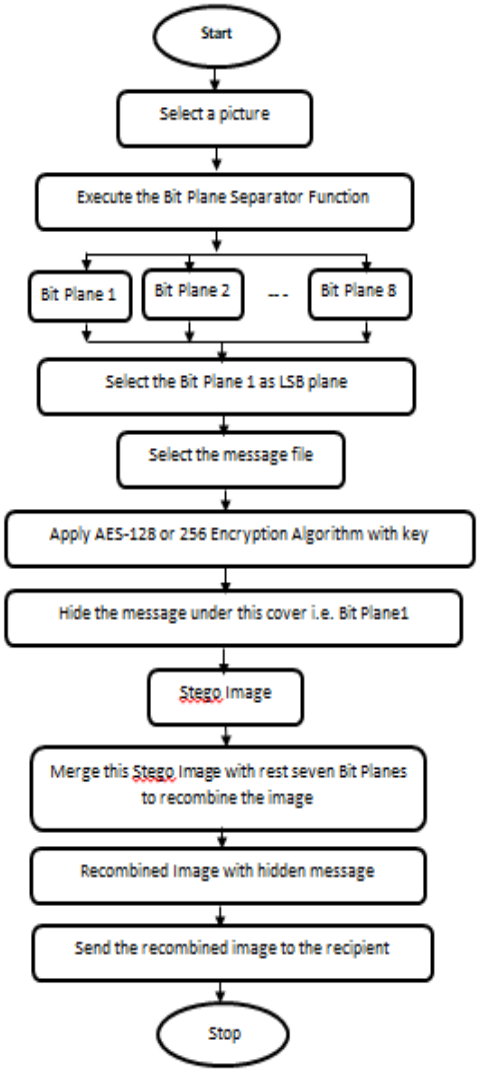

Figure 2: Process Flow chart of LBPSE message Hiding under a LSB cover and embedding the LSB bit plane

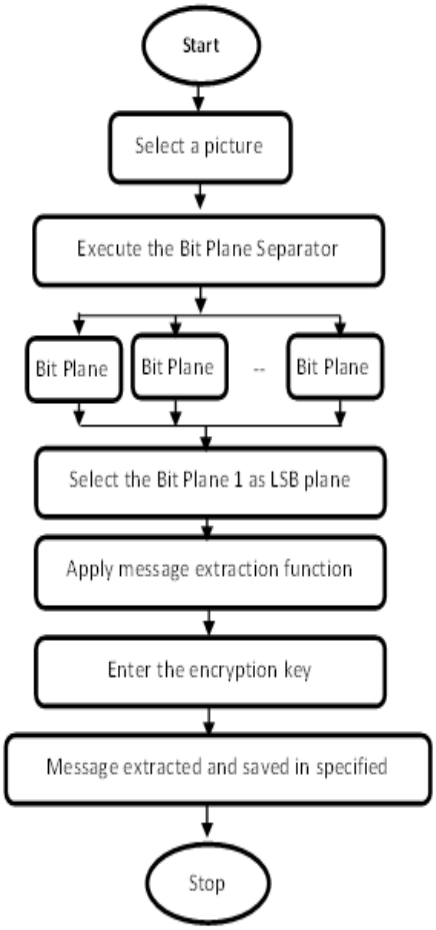

Figure 3: Process Flow chart of LBPSE model for message extraction method from stego image

3. IMPLEMENTATION OF LBPSE MODEL

In this section of the paper, the implementation part of the LBPSE model has been illustrated. As discussed above that the LBPSE model has two part, the first part will perform the steganography and the second part will perform the steganalysis.

In the first part i.e. for steganography, there are three basic requirement of implementing this model LBPSE of secret message communication are: (i) Input image, (ii) message file, and (iii) Secret Key for encryption.

So, we first take a grey scale image say "pic1.png" shown in figure 4 and then separated all the eight bit planes of this image as Bit Plane 1-8, as illustrated in the figure 5.

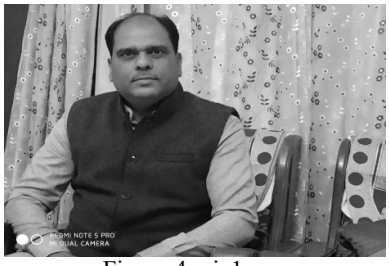

Figure 4: pic1.png

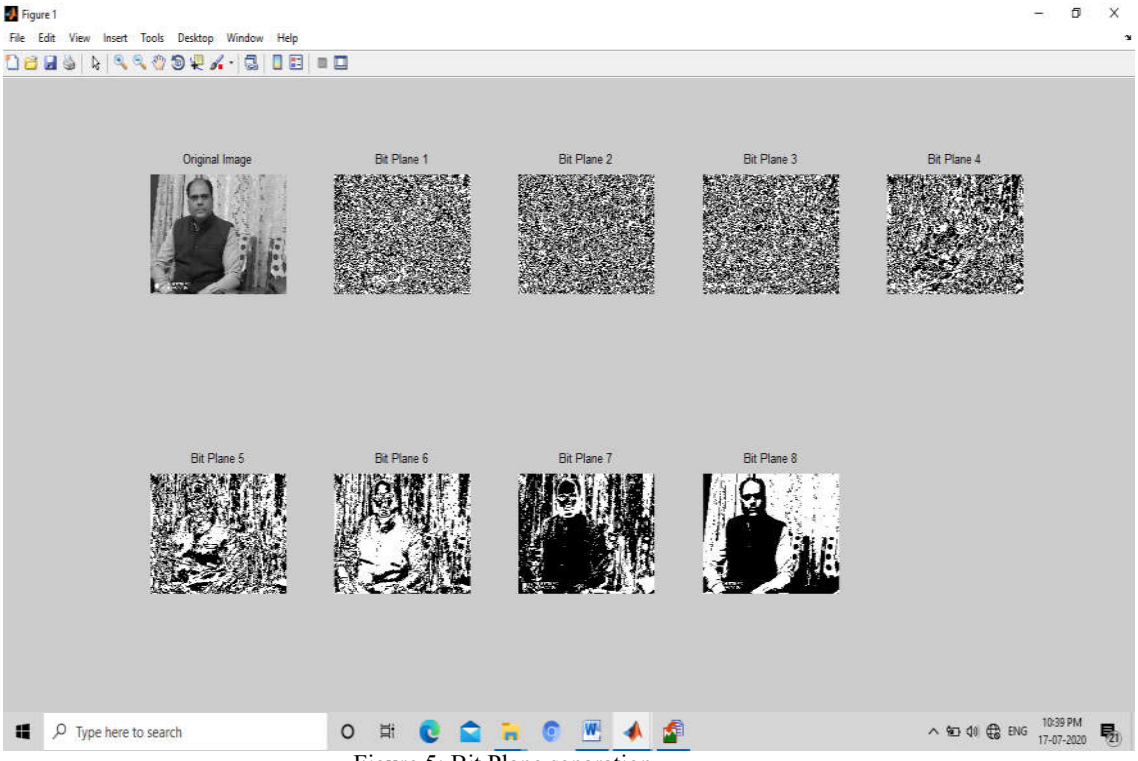

Figure 5: Bit Plane separation

Bit Plane 1 is the LSB plane and we use this plane as cover image for hiding the message, the Bit Plane 1 is shown in figure 6 and message is stored in a text file, for example "message.docx", as shown in figure 7.

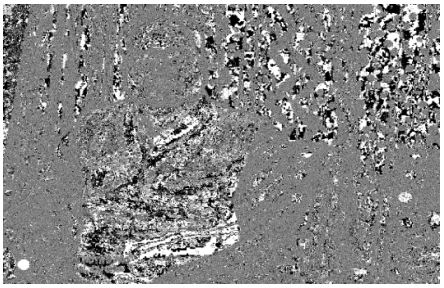

Figure 6: Bit Plane 1

Steganography is an art of hiding secret message under a cover. This cover may be a text, image, audio, or video. Now using this steganography let us hide a message under an image cover. We may use a plain image either jpg, png,, or any other. We will use LSB of the given image for improving security of message. Here, the secret key is ALFA ALFA. This secret key should be kept confidential and will explain the secret plan of the success.

Figure 7: Message.docx

To more secure the message, we then applied the AES-128 encryption method on this message before hiding the message and hided the encrypted message under the LSB cover and the outcome is the stego image, as shown in figure 8.

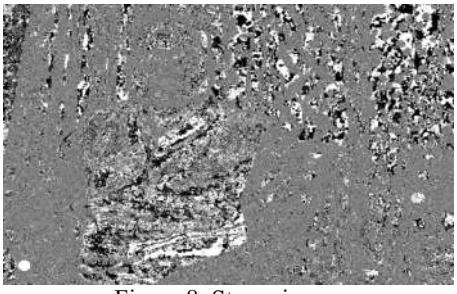

Figure 8: Stego_image

In the next step, this stega image will be merged with the rest seven bit planes i.e. from Bit Plane 2 to Bit Plane 8, that we have separated earlier from the original image i.e. “pic1.png” and the outcome will be called as “recombined image”, as shown in figure 9 as recombined image.

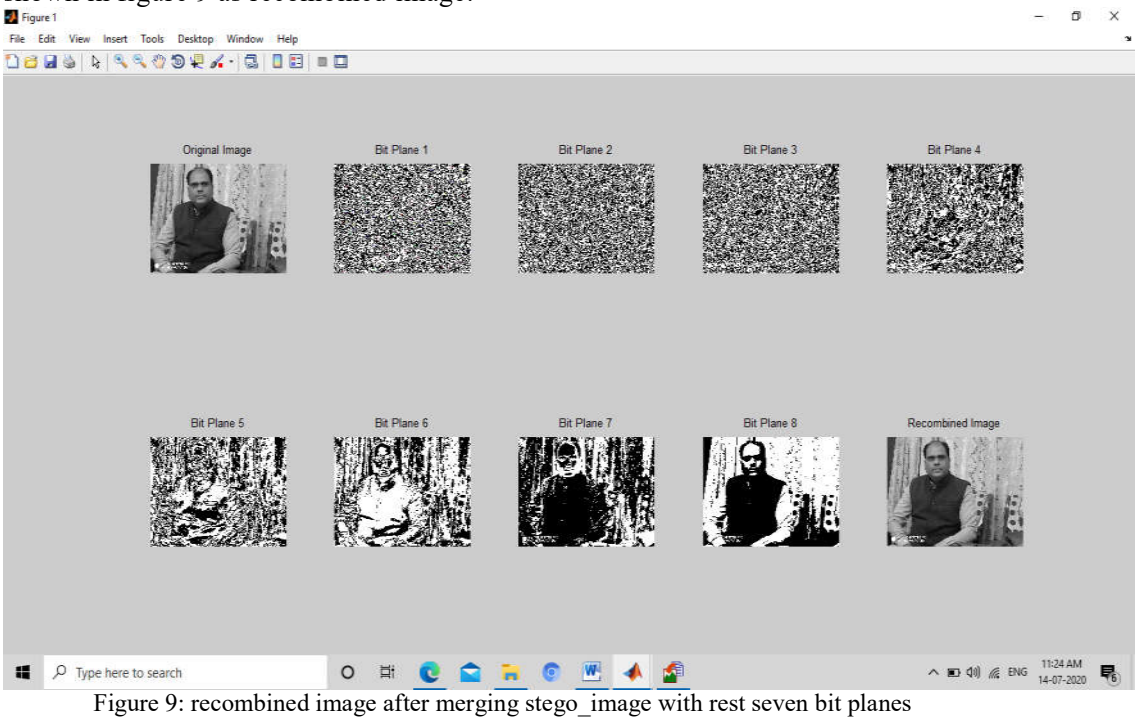

Figure 9: recombined image after merging stego_image with rest seven bit planes

Now, this recombined image is the outcome of the first part of the LBPSE model and this image will be ready to send the message secretly under the cover image file. When the receiver receives this image, it will first separate all the bit planes and select the Bit Plane 1, as this is the main stego_image having the secret message. In the next step, execute the message extraction ( ) method of LBPSE model to obtain the hidden message. This whole process is shown in the figure 10.

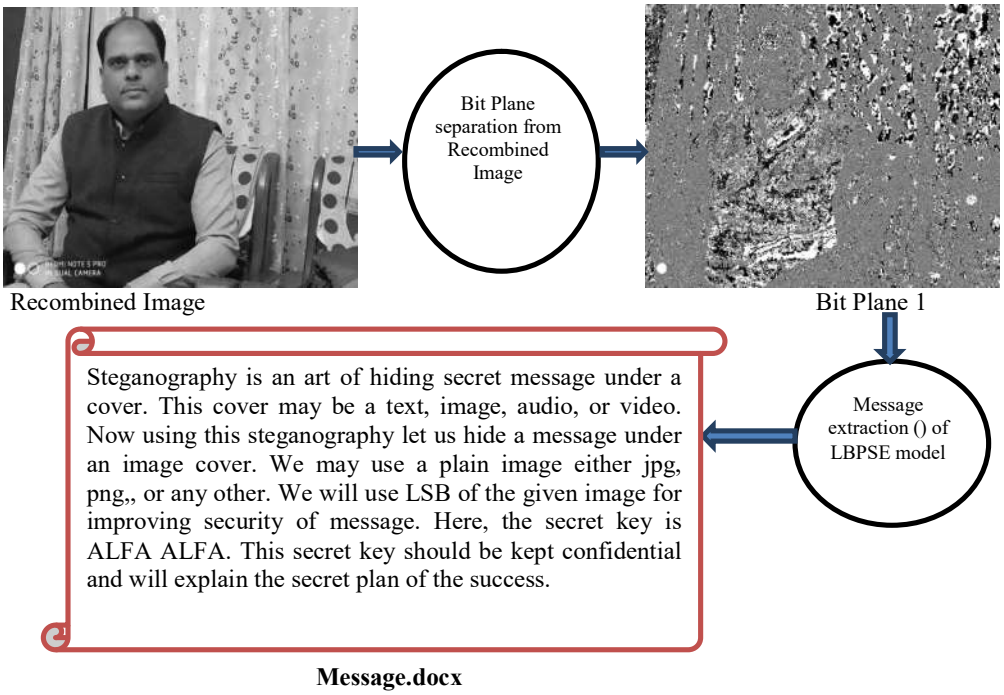

Figure 10: Bit plane separation and message extraction process of LBPSE

4. CONCLUSION

As shown in the section 2 and 3 of this paper, the LBPSE is an innovative model for message hiding and doing communication with confidentiality. There are zero chances of information leak, the application of encryption algorithm AES will improve the level of confidentiality. The AES is available in this model with its two forms: (i) AES-128, and (2) AES-256. In AES-128, the secret key may be of 16 characters, whereas in AES-256, the secret key may be of 32 characters and we may use different complex key combinations for making the security level more high.

The implementation and understanding of the LBPSE model is simple to understand but is very complex and strong to break in reality. So, it is good and innovative model for secret message communication and such systems are more required in the situation arises like covid-19 pandemic for communication through internet like medium using different communication application software.

Acknowledgments

Secure message communication using the application of LSB image is really very interesting. Developing the innovative approach by separating bit planes and application of AES encryption algorithm for encrypting the message in LSB image and then

recombining the bit planes is a tough task. The authors are thankful to all the contributors for their valuable support for making it successful.

REFERENCES

[1] *J. K. Mandal and Debashis Das, "Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain", International Journal of Information Sciences and Techniques, volume 2,2012, pp.83-94.*

[2] *Abdelhamid Awad Attaby, Mona F.M. Mursi Ahmed, Abdelwahab K. Alsammak, "Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3", Ain Shams Engineering Journal,2017, pp.1-12*

[3] *Abhijeet Bhaskar, Mr. Upendra Kumar Acharya "IMAGE STEGANOGRAPHY USING MODIFIED LSB",2013, pp.1-5*

[4] *Mohammad Alia and Khaled Suwais, "Improved Steganography Scheme based on Fractal Set", The International Arab Journal of Information Technology, volume 17,2017 ,pp. 128-137*

[5] *Akash Nag, "Low-Tech Steganography for Covert Operations", Modern Education and Computer Science press, volume 1,2018,ISSN:18-30,pp.18-30*

[6] *Biswajita Datta Upasana Mukherjee , Samir Kumar Bandyopadhyaya, " LSB Layer Independent Robust Steganography using Binary Addition", Elsevier, vol.18, 2016, ISSN: 425-432, pp. 425-432*

[7] *Ashita and Smitha, "RANDOMIZED STEGANOGRAPHY IN SKIN TONE IMAGES", International Journal of Computer Science, Engineering and Information Technology (IJCSEIT),volume 8, 2018, pp.1-9*

[8] *P. Malathi, T. Gireesh kumar, " Relating the embedding efficiency of LSB Steganography techniques in Spatial and Transform domains", Elsevier, vol. 93, 2016, ISSN: 878-885, pp. 878-885*

[9] *A. Antony Raj, M. Vickraman, A. Vishnu, M. R. Mahalakshmi, "Secure RGB Image Steganography based on Fused Distortion Measurement", International Journal of Research in Engineering , Science and Management ,volume 2,2019,ISSN:2581-5792,pp.175-178*

[10] *Gija Susan Issac ,Jobi Jose, "Secured Transmission Of Image/Video By Performing Reversible Color Transformation", Elsevier, volume 24, 2016, issn:1032-1038, pp. 1032-1038*

[11] *Avinash Sharma, Rajendra Kumar Buraniya, Prashant Kumar Singh, "STEGANOGRAPHY: AN OVERVIEW", International Journal For Technological Research In Engineering ,volume 6,2019,ISSN:2347-4718,pp.5084-5086*

[12] *Ghania Al Sadi, "Image Steganography Approach", International Journal of Computer Science and Mobile Computing, volume 4, 2015, ISSN:2320-088X, pp.166-169*

[13] *Ammar Odeh, Khaled Elleithy, Miad Faezipour, "Steganography in Text by Using MS Word Symbols", Proceedings of 2014 Zone 1 Conference of the American Society for Engineering Education, 2018, pp.1-7*

[14] *Amrita Khamrui, J K Mandal, "A Genetic Algorithm based Steganography using Discrete Cosine Transformation", Elsevier, volume 10, 2013, ISSN: 105-111, pp. 105-111*

[15] *Daphney Jerly, Dsouza Girish S, "A method of data hiding in QR code using image steganography", INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS*

AND INNOVATIONS IN TECHNOLOGY, volume 4, 2018, ISSN: 2454-132x, pp.1111-1113

[16] *Della Babya, Jitha Thomasa, Gisny Augustinea, Elsa Georgea, Neenu Rosia Michaela," A Novel DWT based Image Securing Method using Steganography", Elsevier, volume 46, 2015, ISSN: 612-618, pp.612-618*

[17] *Gandharba Swain , " A steganography method combining LSB substitution and PVD in a block ", Elsevier, volume 85, 2016, ISSN: 39-44, pp. 39-44*

[18] *Ratnakirti Roya, Anirban Sarkara, Suvamoy Changdera, "Chaos based Edge Adaptive Image Steganography", Elsevier, vol. 10, 2013, ISSN: 138-146, pp. 138-146*

[19] *V.Nagaraj, Dr. V. Vijayalakshmi and Dr. G. Zayaraz, "Color Image Steganography based on Pixel Value Modification Method Using Modulus Function",Elsevier ,volume 4, 2013, ISSN: 17-24, pp.17-24*

[20] *Vipul Sharma ; Madhusudan, "Two New Approaches for Image Steganography Using Cryptography", 2015 Third International Conference on Image Information Processing (ICIIP), pp. 202-207*