Literature Review: Information Security A Comparative Analysis of Steganography Algorithms

Mr. Harshal V. Patil[1], Dr. Vaibhav P. Sonaje[2], Dr. B. H. Barhate[3]

[1]Research Scholar, Sandip University Nashik India

[2]Department of Computer Science & Application, SOCSE, Sandip University, Nashik, India

[3]Professor, DOCSIT, Bhusawal Arts, Science & P.O.Nahata Commerce College, Bhusawal, India

Abstract — **Information or data is a very crucial resource to us. Thus securing information becomes more essential. The communication medium through which we send data does not provide data security, so other methods of securing data are required. Information hiding plays a very important role today. It provided methods for encrypting the information to become unreadable for any unintended user. In the last few years, the security of data over the internet has become a very difficult task. With the increasing usage of the internet, the protection of information has become a critical Issue. Information security is one of the most important concerns in any communication. Data hiding is a related field to information security. This has made people worry about their privacy and work.**

Steganography is a technique that prevents unauthorized users from having access to important data. It is the science of hiding the information into the other information so that the hidden information appears to be nothing to the human eyes. In this paper, we review different steganography techniques for data hiding. The purpose of this paper is to present an overview of various information-hiding techniques. A brief history of steganography is provided along with the techniques used to hide information

Keywords — **Steganography, Stego-Key, Stego-File, LSB, BPCP, PVD, DCT, PSNR, MSE, SNR, NCC, BER.**

I. INTRODUCTION

Nowadays, the amount of data exchanged through the internet is increasing. Therefore, data security is recognized as a critical issue when the communication of data is processed over the Internet. Everyone needs their data to be safe during communication [1].

Steganography is defined as the study of invisible communication. Steganography usually relates to hiding the existence of communicated data so that it remains confidential.

"Steganography" is a Greek origin word that means "hidden writing". Steganography word is classified into two parts: Steganos which means "secret or covered" (where you want to hide the secret messages) and the graphic which means "writing" (text). However, in hiding information the meaning of Steganography is hiding text or secret messages into another media file such as image, text, audio, and video. [4].

Steganography is a very old art of embedding personal information into other data using certain rules and techniques. As a result, unauthorized users cannot see and identify the embedded information.

Steganography is managing a secret path for sending information invisibly. Steganography is a useful technique to hide data behind a carrier file such as image, audio, or video, and transmit that data securely from the sender to the receiver. Steganography is the process of hiding a message, audio, image, or video by embedding it in another image, audio, message, or video. It is employed to protect secret data from malicious attacks [2].

Need of Data hiding:

A few reasons behind data hiding are as follows:

* Personal and private data
* Sensitive data
* Confidential data and trade secrets
* To avoid misuse of data
* Unintentional loss of data, human error, and accidental deletion of data
* Blackmailing purposes
* Cybercrime

II. DATA HIDING USING THE STEGANOGRAPHY MODEL

The model for steganography is shown in Fig 1. A message is data that the sender wishes to keep

confidential. Message can be plain text, image, audio, or any file type. Password is known as a stego-key, using the stego key the receiver can extract the message from a cover file if the receiver knows the stego key. The cover file with the secret information is known as a stego-file [4].
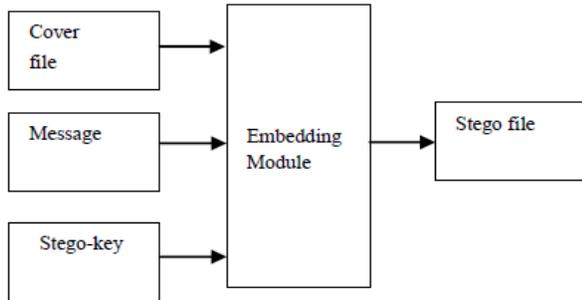
Fig.1 Basic Steganography Model

Basic terms for Steganography

•   Cover-object/File: The original object where the message has to be embedded.
•   Secret Data/Message: The data that is to be embedded in a cover object is known as a secret message.
•   Stego object/File: The cover object, once the message has been hidden or embedded.
•   Stego Key: The secret code to be shared between Sender and receiver to embed and retrieve the message.
•   Embedding algorithm: It is the way or the idea that is often used to embed the secret information in the cover message.

III.   TYPES OF STEGANOGRAPHY

1.   Image Steganography: - For hiding the secret message in carrier image, which is then converted into a stego-image.
2.   Text Steganography: - In this, the message that is to be sent is rooted firstly in a text file by formatting. The format is based on line-shift coding, word-shift coding, feature coding, etc. Reformatting of the text destroys the rooted content hence the technique is not robust.
3.   Audio Steganography:- A secret message is embedded into unused audio bits as every file contains some unused bits or unused areas of bits where a secret message can be hidden.

4.   Video Steganography: - Video steganography divides the video into audio and image frames where embedding is performed in the audio file.
5.   Network Steganography:- It involves hiding the information by taking the network protocol such as TCP, UDP, ICMP, IP, etc., as a cover object. In the OSI layer network model there exist covert channels where steganography can be used.

IV.   CLASSIFICATION OF STEGANOGRAPHY TECHNIQUES

There are following some approaches to classifying the Steganography techniques are given below:

1.   Spatial Domain Methods: In this method, secret data is embedded directly into the pixel intensity. It means some pixel values of the image are changed directly while hiding data. Spatial domain techniques are classified into the following categories:

   i) LSB: This method is most commonly used for hiding data. In this method, embedding is done by replacing the least significant bits of image pixels with bits of secret data. The image obtained after embedding is almost similar to the original image because the change in the LSB of the image pixel does not bring too many differences in the image.

   ii) BPCP: In this segmentation, images are used by measuring their complexity. Complexity is used to determine the noisy block. In this method, noisy blocks of bit plan are replaced by binary patterns mapped from secret data.

   iii) PVD: In this method, two consecutive pixels are selected to embed data.. Payload is determined by checking the difference between two consecutive pixels and it serves as the basis for identifying whether the two pixels belong to an edge area or smooth area.

2.   Spread Spectrum Technique: This technique uses the concept of spread spectrum. In this method, the secret data is spread over a wide frequency bandwidth. Each frequency band must have a signal-to-noise ratio so small that it is difficult to detect the presence of data. Even if parts of data are removed from several bands, there would be still enough information present in other bands to recover the data. Thus it is difficult to remove the data completely without destroying the cover. It is a

very robust technique mostly used in military communication.

3. Statistical Technique: In the technique, the message is embedded by changing several properties of the cover. It involves the splitting of the cover into blocks and then embedding one message bit in each block. The cover block is modified only when the size of the message bit is one otherwise no modification is required.

4. Transform Domain Technique: In this technique; the secret message is embedded in the transform or frequency domain of the cover. This is a more complex way of hiding a message in an image. Different algorithms and transformations are used on the image to hide a message in it. Transform domain techniques are broadly classified as follows:
   Discrete Fourier transformation technique (DFT)
   1) Discrete cosine transformation technique (DCT)
   2) Discrete Wavelet transformation technique (DWT)
   3) Lossless or reversible method (DCT)
   4) Embedding in coefficient bits

5. Distortion Techniques: In this technique, the secret message is stored by distorting the signal. A sequence of modifications is applied to the cover by the encoder. The decoder measures the difference between the original cover and the distorted cover to find the sequence of changes and recover the resulting secret message.

6. Masking and Filtering: These techniques hide information by marking an image. Steganography only hides the information as watermarks become a portion of the image. These techniques embed the information in the more significant areas rather than hiding it in the noise level. Watermarking techniques can be applied without fear of image loss due to lossy compression as they are further integrated into the image. This method is used for 24-bit and greyscale images.

V. FACTORS AFFECTING A STEGANOGRAPHY SYSTEM

The effectiveness of any Stenographic method can be visualized by comparing the Stego Image (Image after inserting the message) with the Cover Image (Image before message insertion). Thus, some factors that determine how efficient and powerful a technique is are as follows.

1) Robustness: Robustness refers to the ability of the embedded data to remain intact if the stego-image changes, such as linear and non-linear filtering, the addition of random noise, sharpening or blurring, scaling and rotation, cropping or decimation, lossy compression.

2) Imperceptibility: The invisibility of a stenographic algorithm is the first and foremost requirement since the strength of steganography lies in its ability to be unnoticed by the human eye. Algorithms are compromised as soon as an image is seen to be tampered with.

3) Payload Capacity: This cover refers to the amount of secret information that can be hidden in the source. Watermarking needs to embed only a small amount of copyright information, on the other side, steganography aims at hidden communication and therefore requires sufficient Embedding capacity.

4) PSNR (Peak Signal to Noise Ratio): It is the ratio between the maximum possible powers of a signal and the power of corrupting noise that affects the fidelity of its representation. This ratio is used as a measure of quality between the original and the compressed image. The higher the PSNR, the better the compressed image quality.

5) MSE (Mean Square Error): Mean Squared Error is the average squared difference between a reference image and a distorted image. An Image steganography technique is efficient if it gives a low MSE. Pixel-by-pixel is calculated by adding the squared differences of all pixels and dividing by the total number of pixels.

6) SNR (Signal to Noise Ratio): It compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to noise power.

7) NCC (Normalized Cross-Correlation): Normalized cross-correlation can be used to determine how to register or align the images by translating one of them. NCC is one of the methods used for template matching, a process used for finding incidences of a pattern or object within an image.

8) BER (Bit Error Rate): The bit error rate or bit error ratio (BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval.

VI. LITERATURE REVIEW

In this research work, we reviewed many papers on steganography techniques. These papers are good enough and have wide future scope. By reviewing these papers we observed that most of the steganography work has been done in the last few years. In these years, LSB has been the most widely used technique for steganography [12].

Soni et al. 2020 [5] Proposed a grayscale medical image encryption technique by hiding the patient information in the form of a 2D barcode into the grayscale medical using the LSB technique and encrypting that grayscale image after hiding the patient information using Genetic Algorithm. İt improve the security of patient information with medical images. Kini et al. 2019 [2], Present the recent enhancements in computer security have shown that concealment of info instead of encoding is the best thanks to shield information. The LSB could be a widely used method of knowledge concealment and is at risk of attack owing to its simplicity. In this, A 24-bit color image carrier is employed to cover the key image and the same is employed to cover the steno key. It compares the PSNR associated suggests that MSE and runs an analysis graph to work out to what level the steno image is hidden within the carrier image. Watni et al. 2019 [6], discussed different steganography techniques that were used previously and gave us a comparative analysis for jpeg image steganography. Benedict et al. 2019 [7], Present the data bits of the message to be veiled are organized arbitrarily and the pixel bits of the picture are likewise made interesting, making the example garbled to recognize. Krishna et al. 2016 [8], Have indicated that the proposed reversible steganography strategy utilizing the pre-prepared DES IMNP calculation permits better joining and picture quality qualities to be contrasted with existing NMI and INP methods. Shelke et al. 2015 [9], the proposed plot limits the distortion after data interpolation. The execution of this plan is straightforward. It is more affordable than the space domain methods recently utilized. The data concealing capacity is more prominent than that of DE and EMD. Mousa et al. 2013 [10], proposed the random function strategy coordinates touchy data into a norm and non-standard host picture utilizing various random coefficients and boundaries. Al-Shatnawi et al. 2012 [11], A DWT-based approach for steganography using biometric features. Here, the secret data is embedded in the skin region of the image providing a secure location for data hiding. Secret data is hidden in one of the high-frequency subbands of DWT by tracing skin pixels. This provides security to the method and PSNR is used to determine the quality of the stego image after embedding the secret data. Menon et al. 2017 [13], Discussed several areas, Security systems are extremely popular as technology grows each day. By using secret writing and concealing info, info security is achieved. Within the times, text secret writing is most frequently related to the encoding of unencrypted text in encrypted text, then back. Within the presence of third parties, this can be an observer of secure communication. Gedkhaw et al. 2018 [14], Discussed protecting info using hidden info as the art and science of writing a hidden methodology of hidden knowledge in several sorts of data to cover data. Shankar et al. 2016 [15], Discussed that digital image extraction has several applications within the field of knowledge and communication security. Hidden knowledge in encrypted pictures ensures that the quilt image and confidential message will be retrieved by the recipient.

Nag et al. 2011 [16], discussed and presented Steganography as an art of activity the existence of communication, as well as confidential messages in innocent and harmless incidental to documents, like digital pictures, video, and audio files. Here they tend to gift a replacement methodology of planning hidden info supported by the LSB algorithmic program to ensure reliable security and intangible visual quality of a confidential message. Signh et al. 2018 [17], presented the Information that the wealth of any organization, and within the gift era, once data is transmitted through digital media and also the net, it's become a high priority for any establishment to guard this wealth. Steganography is one such manner in which a confidential message cannot be detected, and that will be used as a security tool to firmly transmit direction. This work aims to match LSB with the planned separate distinct wave conversion algorithmic rule (DWT). The smallest amount of important bit insertion (LSB) methodology could be a spatial field method within which pixels are processed within the cowl image to incorporate sensitive data. Prashanti et al. 2015 [18], Discussed that Steganography is the art of activity information on a medium in such the simplest way that data can't be detected throughout data exchange. This gives the summary of the newest advances in LSB-based data concealment that have the final word goals of up information concealment: undetected ability, responsibility, and capability of hidden information.

Some researchers have also used techniques like watermarking, distortion technique, spatial technique, ISB, and MSB in their work and provided a strong means of secure information transmission. These papers provide a lot of help to beginners in starting their work in this field. The different security and data hiding techniques are used to implement steganography using LSB, ISB, and MLSB.

VII. COMPARATIVE STUDY OF STEGANOGRAPHY ALGORITHMS

Ref. No.	Year	Techniques Used	Description	Advantage
[19]	2019	Spatial domain	In this, give an overview of the different image steganography techniques.	In this, achieved the better quality of the stego image in terms of robustness and better security.
[12]	2019	LSB	This gives the details about how the secret image is hidden in the 24-bit color cover image using the LSB technique.	Gives an enhanced hiding technique that is difficult to crack easily.
[20]	2019	Watermarking, fingerprinting, cryptography, steganography techniques	Gives an overview of data-hiding techniques in a digital cover image.	In this, various data hiding techniques were investigated to improve the system's hidden effectively
[21]	2018	LSB substitution and QVD	Presented the data hiding technique in images with higher embedding capacity using a combination of LSB substitution and QVD.	In this experiment, it is evidenced that the hiding capacity is improved to a greater extent.
[22]	2018	DCT, DWT, and CvT	In this, use the RGB image as a cover image to hide the secret data. secret information is hidden in a red (R) color channel to ensure the best recovery of embedded information	In this, the poison noise gives better results than other noise.
[23]	2018	Spatial domain-LSB	A genetic scheme for detecting the optimum regions from the cover image is used then a secret bit embedded randomly based key using steganography based on LSB replacement	A higher state of an imperceptible number of stenographic techniques are used to increase security.
[24]	2017	DCT, DWT, LSB	Given an overview of steganography to embed secret information from the sender to the receiver with the image as its cover to embed or secure.	Security of the data that we talk with other people is important to be protected with the use of steganography.
[25]	2017	LWT, DWT, SVD	In this, two approaches of steganography based on LWT- DCT-SVD and LWT-DWT-SVD is suggested. These proposed steganography algorithms use LWT, DWT, DCT, and SVD transformation which contribute more Robustness in comparison with many steganography algorithms.	Steganography algorithms using LWT, DWT, DCT, and SVD transformation that contribute more robustness in comparison with many steganography algorithms.
[26]	2016	DCT, DWT And SVD	This presents numerous stenographic techniques that have been recently proposed for hiding the secret data within the cover images efficiently.	Imperceptibility, Robustness
[27]	2016	K-Means Clustering and Encryption Techniques	Image steganography allows two individuals to communicate privately. This proposed a method using this technique to securely send sensitive information without worrying about man-in-the-middle attacks.	The encrypted text is hidden in each of the clusters which further diminishes the probability of the message being found.

[28]	2016	LSB, ILSB	In this, provide three levels of security, rather than hiding the message bits directly in cover image, pixels are generated randomly through a pseudo-random number generator after that secret data is hidden behind a cover image using the inverted LSB method	Gives higher PSNR and lower MSE values.
[29]	2015	ILSB	Introduced a new image steganography using LSB encoding with two primary objectives.	To achieve better security, it is crucial to select a proper cover and secret.
[30]	2015	LSB	This, presented two improved approaches over the classical LSB technique.	The proposed technique is applied in a grayscale and gets a high PSNR value.
[31]	2014	DCT	In this, proposed a novel digital image watermarking algorithm based on DCT and spread spectrum	This algorithm provides statistical security and robustness against various attack
[33]	2013	Hash-LSB	For hiding data bits in LSB used a hash function.	This hash-LSB increases the security of secret messages.
[34]	2012	LSB and DCT	This is used to maximize the storage capacity compression algorithm.	It works efficiently for .bmp images.
[36]	2012	Modified LSB	Searching for identical bits hides the secret data.	More efficient, simple, appropriate, and accurate.
[37]	2012	DWT	In detecting the most important regions in the cover image, the method called Speeded Up Robust Features is used.	Even if the image is modified by the attacks, The SURF can be used to identify the points.

Table 1: Comparative Analysis of Different Previous Work Done on Different Steganography Techniques

VIII. CONCLUSION

This paper reviews steganography, the need for steganography, the Classification of steganography and its techniques, and factors of steganography design.

In this, many important stenography techniques have been introduced and analyzed to become familiar with the different stenography algorithms that are used for the image that has been transferred to the network. According to the survey of recent research, it has been said that security is the main concern in transmitting images. Stenography sends privileged insights through apparently innocuous covers to hide the presence of a secret. Hide advanced data, images, and their subordinates is progressively utilized and applied. This gives an overview and comparative analysis of different stenography techniques for image, data, or information hiding.

By reviewing these papers we saw that most of the steganography work was done in 2012 and 2013. In recent years, LSB has been the most widely used technique for steganography. Some researchers have also used techniques like watermarking, distortion technique, spatial technique, ISB, and MSB in their work and provided a strong means of secure information transmission. These papers help a beginner a lot to start

their work in this field. This review paper is enough for them to start working in this field. The different security and data hiding techniques are used to implement steganography using LSB, ISB, and MLSB. In further research, we are going to use more advanced schemes like steganography with some hybrid cryptographic algorithms for enhancing data security.

REFERENCES

[1] Gaurav Kumar Soni, Himanshu Arora, and Bhavesh Jain, "A Novel Image Encryption Technique Using Arnold Transform and Asymmetric RSA Algorithm", In. Springer International Conference on Artificial Intelligence: Advances and Applications 2019, Algorithm for Intelligence System, 89-90 (2020).

[2] N. Gopalakrishna Kini, Vishwas G. Kini and Gautam, "A Secured Steganography Algorithm for Hiding an Image in an Image.", In. Springer Nature Singapore Pte Ltd., Integrated Intelligent Computing, Communication and Security, Studies in Computational Intelligence 771, 539-546 (2019).

[3] Imra Aqeel and Muhammad Babar Suleman, "A Survey on Digital Image Steganography

Approaches" In Springer Nature Singapore Pte Ltd. INTAP, CCIS 932, 769–778 (2019).

[4] R. Anderson and F. Petitcolas, "On the limits of Steganography" IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, (1998).

[5] G. K. Soni, A. Rawat, S. Jain and S. K. Sharma, "A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm with LSB Watermark Technique", in Smart Systems and IoT: Innovations in Computing: Springer. pp. 483-492, 2020.

[6] Dipti Watni and Sonal Chawla, "A Comparative Evaluation of Jpeg Steganography", 5th IEEE International Conference on Signal Processing, Computing, and Control (ISPCC 2k19), 36-40, (2019).

[7] Vipin Singh, Manish Choubisa and Gaurav Kumar Soni, "Enhanced Image Steganography Technique for Hiding Multiple Images in an Image Using LSB Technique", TEST Engineering & Management, Vol-83, PP-30561 - 30565, May-June 2020.

[8] Dr. Himanshu Arora, Mr. Manish Kumar, and Mr. Sanjay Tiwari, "Improve Image Security in Combination Method of LSB Stenography and RSA Encryption Algorithm", International Journal of Advanced Science and Technology, Vol-29, No-8, 6167-6177, (2020).

[9] S.G..Shelke and S.K.Jagtap, "Analysis of Spatial Domain Image Steganography Techniques", In. IEEE International Conference on Computing Communication Control and Automation, 665- 667 (2015).

[10] Hamdy M. Mousa, "Secured Steganography Algorithm Based Random Function", 2013 8th International Conference on Computer Engineering & Systems (ICCES), 228-232 (2013).

[11] Atallah M. & Al-Shatnawi, (2012) A New Method in Image Steganography with Improved Image Quality, Applied Mathematical Sciences, 6, pp. 3907-391.

[12] N. F. Johnson, S. Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE Computer vol. 31, issue 2, pp. 26-34, 1998.

[13] Nidhi Menon and Vaithiyanathan, "A Survey on Image Steganography", 2017 IEEE International Conference on Technological Advancements in Power and Energy (TAP Energy), PP-1-5, 2017.

[14] Eakbodin Gedkhaw, Nantinee Soodtoetong, and Mahasak Ketcham, "The Performance of Cover Image Steganography for Hidden Information

within Image File using Least Significant bit algorithm", IEEE The 18th International Symposium on Communications and Information Technologies (ISCIT 2018), PP- 504-508, 2018.

[15] Siva Shankar S and A. Rengarajan, "Data Hiding In Encrypted Images Using Arnold Transform", ICTACT Journal On Image And Video Processing, Volume-07, Issue-01, PP-1339-1344, August 2016.

[16] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar, and Partha Pratim Sarkar, "A Weighted Location Based LSB Image Steganography Technique", Springer-Verlag Berlin Heidelberg 2011, ACC 2011, Part II, CCIS 191, pp. 620–627, 2011.

[17] Akanksha Singh, Monika Chauhan, and ShilpiShukla, "Comparison of LSB and Proposed Modified DWT Algorithm for Image Steganography", IEEE International Conference on Advances in Computing, Communication Control and Networking (ICACCCN2018), PP-889-893, 2018.

[18] G. Prashanti and K. Sandhyarani, "A New Approach for Data Hiding with LSB Steganography", Springer International Publishing Switzerland 2015, Emerging ICT for Bridging the Future − Volume 2, Advances in Intelligent Systems and Computing 338, PP-423-430, 2015.

[19] Imra Aqeel and Muhammad Babar Suleman, "A Survey on Digital Image Steganography Approaches", Springer INTAP 2018, CCIS 932, pp. 769–778, 2019.

[20] Jagadish Gurrala and Pasala Sanyasi Naidu, "A Secure Framework for Communicating Multimedia Data in Cover Images using Hybrid Steganography Algorithms in Wireless Local Area Network", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-9 Issue-2S3, pp-35-43, December 2019.

[21] Gandharba Swain, "Very High Capacity Image Steganography Technique Using Quotient Value Differencing and LSB Substitution", Springer Arabian Journal for Science and Engineering, pp-1-10, June 2018.

[22] Wisam Abed Shukur, Wathiq Najah Abdullah and Luheb Kareem Qurban, "Information Hiding In Digital Video Using DCT, DWT and CvT", Journal of Physics: Conference Series 1009, pp-1-19, 2018.

[23] Prat K D. Shah, Bichkar RS, "A Secure Spatial Domain image Steganography Using Genetic

Algorithm and Linear Congruential Generator", International Conference on Intelligent Computing and Application, Advances in Intelligent Systems and Computing, 2018.

[24] Aryfandy Febryan, Tito Waluyo Purboyo and Randy Erfa Saputra, "Steganography Methods on Text, Audio, Image and Video: A Survey", International Journal of Applied Engineering Research ISSN 0973- 4562 Volume-12, Number-21, pp-10485-10490, 2017.

[25] Shallu Vohra and Binay Binod Kumar, "Image Steganography Using Hybrid Method LWT-DWT-SVD", International Journal of Innovative Research in Science, Engineering and Technology, Vol-6, Issue-8, August 2017.

[26] Wafaa Mustafa Abdullah and Abdul Monem S. Rahma, "A Review on Steganography Techniques", American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS), PP-131- 150, 2016.

[27] Bhagya Pillai, Mundra Mounika, Pooja J Rao and Padmamala Sriram, "Image Steganography Method Using K-Means Clustering and Encryption Techniques", 2016 Intl. Conference on Advances in Computing, Communications and Informatics (ICACCI),pp-1206-1211, Sept. 21-24, 2016.

[28] Rupali Bhardwaj and Vaishali Sharma, "Image Steganography Based on Complemented Message and Inverted bit LSB Substitution", Elsevier Science Direct 6th International Conference On Advances In Computing & Communications, ICACC 2016, PP-832-838, 6-8 September 2016, Cochin, India.

[29] Prasenjit Das and Nirmalya Kar, "ILSB: Indicator-Based LSB Steganography", Intelligent Computing, Communication and Devices, Advances in Intelligent Systems and Computing 30, pp-489-495, 2015.

[30] Savita Goel, Shilpi Gupta, and Nisha Kaushik, "Image Steganography – Least Significant Bit with Multiple Progressions", 3rd International Conference on Front. of Intell. Comput. (FICTA), Vol. 2, Advances in Intelligent Systems and Computing 328, pp-105-112, 2015.

[31] Harsh Vikram Singh, Ashutosh Kumar Singh, Suman Yadav, and Anand Mohan, "DCT-based Secure Data Hiding for Intellectual Property Right Protection", Springer CSIT, pp-163-168, November 2014.

[32] Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath. "A secure and high capacity image Steganography technique" Signal & Image Processing", An International Journal (SIPIJ) Vol.4, No.1, February 2013.

[33] Kumar and R. Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", International Journal of Advanced Research in Computer Science and Software Engineering, vol-3, pp-363-372, 2013.

[34] G. Kaur and A. Kochhar, "A Steganography Implementation based on LSB and DCT", International Journal for Science and Emerging Technologies, vol-4, pp- 36-41, 2012.

[35] Gowtham Dhanarasi and Dr .A. Mallikarjuna Prasad, "Image steganography using block complexity analysis", International Journal of Engineering Science and Technology (IJEST) Vol.-4, No-07, July 2012.

[36] A.M.AL-Shatnawi, "A New Method in Image Steganography with improved Image Quality", Applied Mathematical Sciences, vol-6, pp-3908-3915, 2012.

[37] Hamd N, Yahya A, Ahmad AB, Al-Qersh O, "Characteristic Region Based image Steganography Using Speeded-Up Robust Features Technique", International Conference on Future Communication Networks, 2012.