As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 8(04):458-465, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0804077
Available online at: http://www.ijmtst.com/vol8issue04.html

A New Secure Lsb-Based Image Steganographical Approach for Secure Data in Cloud Environment

P.Venkata Hari Prasad[1] | Dr.K.Gangadhara Rao[2]

[1]Research Scholar, Department of CSE,Acharya Nagarjuna University
[2]Professor, Department of CSE,Acharya Nagarjuna University
Corresponding Author Email ID: p.venkatahariprasad@gmail.com

To Cite this Article
P.Venkata Hari Prasad and Dr.K.Gangadhara Rao. A New Secure Lsb-Based Image Steganographical Approach for Secure Data in Cloud Environment. International Journal for Modern Trends in Science and Technology 2022, 8(04), pp. 458-465. https://doi.org/10.46501/IJMTST0804077

Article Info
Received: 25 March 2022; Accepted: 22 April 2022; Published: 27 April 2022.

ABSTRACT

Cloud computing is a robust, adaptable, and economical platform for offering consumer IT services through the Internet. Numerous services are offered by cloud computing to various industries, including medical, IT, and others, and it is rapidly growing at the moment. However, because the majority of the services are managed by third party vendors, certain crucial information is also retained by third parties, making cloud computing more vulnerable than other types of computing.Steganography is the one of the popular and dynamic technique for hiding sensitive information or data within a image, video, audio hence the sensitive data is protectable by unwarranted persons. In this technique, it is planned to include number of methodologies to propose a new technique for gray and color images to produce better results with respect to efficiency and payload capacity. In this proposed technique first we have to obtain codeword with sensitive secret data with the help of its checksum, then the produced codeword is compressed with the suitable compression algorithm before encrypting, then it is added to the header and then inserted into the original image. To embed each byte of data combination of different LSB and MSB of the selected pixels is identified. The proposed method is evaluated and examined with various types of images of different sizes and it provides better results compared to various existing algorithm. The proposed algorithm produces better PSNR(Peak Signal to Noise Ratio, MSE (Mean Square Error), Average difference(AD), Maximum difference(MD), Normalized absolute error(NAE), Cross – correlation(CC) values for different embedding rates of 10%,30% and 50% and also it produces better PSNR and MSE values with respect to sequential LSB algorithm.

Keywords: *LSB Image Steganography, Encryption, Compression, Checksum*

1. INTRODUCTION

These days, it is not advised to save confidential or sensitive information on a person's desktop or on an organization's main server. Everybody stores their personal info in the cloud these days. The word "cloud computing" is well-liked and in-demand. It offers a wide range of services to various industries. Because the data is coming from many sources and different people or clients, maintaining security for client data is an usual and focused word in this setting. Many innovative methods are being presented to protect data, and at first, cloud service providers are also offering some of the fundamental security algorithms. Steganography is also one of the most crucial methods in those security strategies for preventing unauthorised access to sensitive or secret data.Data Security is one of the important

aspects in every field and secure communication with other parties is also one of the main aspect in data communication. Steganography is the one of the popular prominent technique to provide security for secret data from unauthorized parties or third party vendor. This is available in different formats like image steganogarpghy, video steganography and audio steganography also it is applicable in different domains like spatial domain, frequency domain and temporal domain. In that two different domains are present to protect the secret data in an original carrier image or in a carrier file. Most of the existing algorithms are based on the spatial domain. In spatial domain environment the data was static and it is static in nature. In frequency domain environment the data is in dynamic in nature. This study is related to spatial domain in this it deals with LSB and MSB bit of the carrier image and also the secret data. Image steganography have different objectives like capacity, robustness, PSNR and MSE. Capacity is related to size of the secret data which will embed in the carrier image.Figure 1 shows various types of available steganography techniques for spatial and frequency domains.

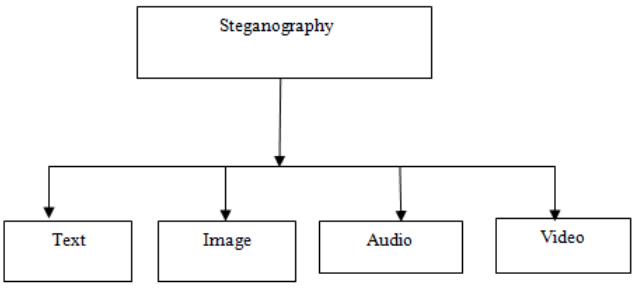

Figure 1: Types of steganography techniques

The rest of the paper is set up as follows. The spatial domain is the subject of the literature study in section 2. Basic ideas pertaining to the suggested methods are provided in section 3. The suggested method's associated algorithms are provided in section 4. Performance comparisons with other existing algorithms are provided in section 5. At the end of the chapter, the conclusion is discussed..

2. LITERATURE REVIEW:

In this presented brief information about various existing techniques in image steganography domain belongs to spatial domain environment [22]. Therefore the proposed technique is related to spatial domain and using LSB, MSB bits for embedding sensitive secret data.

The sensitive original data is immediately placed into the cover image's LSB pixel in the programmes Chanhey Ci-ki and Chengalu C-ms [1]. In this method, find the LSB of the original carrier picture first. Secure data is directly embedded in those chosen pixels[13][14]. With regard to the image's capacity and efficiency, this approach generated improved PSNR and MSE values.

The [16][17] three bit substitution approach is one of the image steganography techniques. One of those three bits, which we choose, is referred as as the ideal pixel. We choose an adjacent pixel based on the ideal pixel, and we employ that one to conceal sensitive information.

In 2016, Akhtarfd Ng [5][18] suggested a change to the LSB substitution method. The inversion notion is used. In those techniques, the PSNR and MSE values include hidden information. Particularly in this inversion technique, some of the source picture's LSB pixels are changed to match the acquired image pattern[19].

Another technique to hide the secret data in pixel based dereferencing method. In this the original method [6][20] was partitioned into block of non overlapping. The difference was calculated from two consecutive pixels of an image. For payload selection the calculated pixels are used .

The randomization is one of the improved techniques in steganography. It works on the basis of reaction of human eyes.In kukapalli[2] have proposed an enhancement in image steganography method. This technique is called pixel Indicator method. In this technique three MSB bits three LSB bits are considered and also use Blowfish algorithm for encrypting the data.

Dighle[3] proposed another improvement in data hiding in an image. In this the secret data embedded by using data parity. In Bash etal presented an improved version in inserting a data in an image under spatial domain environment. This method using four algorithm, Blowish algorithm for encryption and LZW compression. This algorithm produces a better payload capacity and improvement in the quality of the stego image.

In Dadgostar [4]using edge detection algorithm is interval valued edge detection algorithm to insert the sensitive information or data in edge pixels of the original image. This algorithm produces better quality of the stego image.

Some of the steganography algorithms insert data in the Fibonacci pixels of the original image and provides a better results with respect to the PSNR and MSE values[7][8]. In Dr.Kiran kumar proposed a novel approach for inserting the data into the carrier image using steganography and artificial neural networks techniques using secret key embedding[9][10].

In Chandramouli, Rajarathnam [11][12] proposed a new algorithm based on LSB image segmentation techniques and also uses DES and Triple DES algorithm for encrypting original data into cipher text.In Horspool [15] using hide and seek technology for embedding data into an image using image steganogrphy technique it proposed a better results.

A new algorithm for picture segmentation was put forth by Kiran[23] in order to incorporate secret information into images. Before embedding the data, the image is separated into 9 identical portions and the masking method is applied. The original image is translated into the differential image once the masking technique has been applied. Apply the clever edge detection technique after splitting the original image into 9 equal halves, and then choose the Fibonacci edge pixels to insert an image.

In order to insert the data into an image, Suneetha[24] suggested a novel approach in a spatial domain context. An innovative neural network technique built on the cascade feed forward network has been included to this algorithm. In terms of PSNR and Mean Square Error value, it results in superior performance.

Nasir Memon using LSB based image stegonagraphy technique to insert the secret data into an image[25]. Patil, Priyadarshini, et al[26] proposed a new algorithm in combination with three existing algorithms DES,AES and triple DES algorithms to secure secret sensitive data into an image. Mohammad Shkoukani [27] using a new algorithm in combination with genetic and blowfish algorithm it also produce better PSNR and MSE values with various existing algorithms.

3. PROPOSED METHOD DESIGN:

This method consists of two different phases

1. Embedding phase
2. Extraction phase

The embedding process happens on the server. The newly generated data is encoded and compressed using the old data, and then it is integrated into the original cover image. the step of extraction, which happens on the receiving end. The original secret data is extracted from the stego image using it. Every element, word, and idea required for the development of our suggested method is presented in this part.

Integrity of data:

Image Steganography have different objectives one of the main objective of steganography is the robustness or strangeness of the algorithm. When an authorized person wants to manipulate the original image there was a loss of secret data. In this proposed algorithm payload is embedded with the receiver side to identify the data manipulation or to provide the concept of data integrity.

To implement data integrity in this proposed algorithm uses a famous well know technique Cyclic Redundancy check algorithm is used. The CRC technique is a very fast light weight algorithm and can provide a better assurance for integrity of the data. In this process the sender calculate 32 bit length checksum for original secret data and append this checksum to the orginal codeword. In general the checksum length is equal to the codeword length 32 bits at the receiver side after receiving the codeword the last four bytes are separated after that the new checksum is calculated for the remaining bits. Finally compare those two modification was done orginal image was rejected by the receiver.

Compression:

The aim of image steganography is to enhance the capacity of payload and also reduce the probability for chances of identifying the original message from an image.In this the data is hidden into the image and then that image is compressed before storing data into the required environment or before transfer the data to receiver side. In this the sender compresses the sender side codeword and decrypt at the receiver side.

Data Encryption:

The proposed method consist o two level securities. In first level to protect the original secret message from unauthorized persons first we encrypt the original message AES(Advanced Encryption Standard) encryption algorithm .This AES algorithm works with either 128/256 length.

Header:

In this proposed method the new header information system is introduced. This header is used to ensure the secret to embed secret data properly. The sender is responsible for generating 4 bit header information. In this the first 2 bits are used to identify the type of data and the remaining two bits are used to identify the length of the data. The Header format is shown in Figure 2

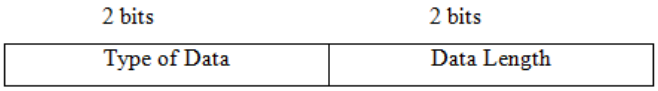

Figure 2: Header Format

Pixel Selection:

One of the important or major aspects of embedding is the pixel selection or selecting pixels. In this proposed method a new algorithm with pseudo random approach is implementing to insert the sensitive secret data. The proposed technique is identifying the dimensions of the cover image for any image has multiple dimensions .Multiple dimensions have multiple pixel values. Among those multiple pixel values select random pixel values using proposed algorithm for hiding secret data.

Proposed Model: The Proposed Model shown in Figure 3

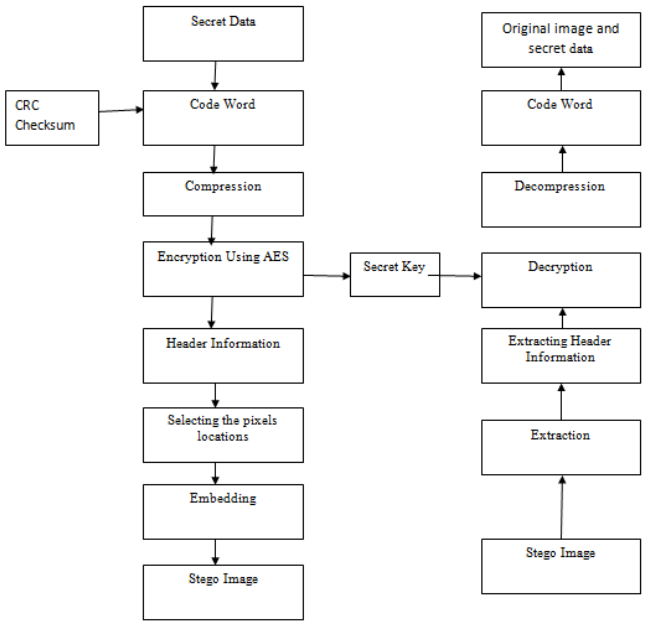

Figure 3: Proposed Model

4.PROPOSED ALGORITHM:

In this section presented proposed algorithm for embedding secret massage and extraction of secret message.

Embedding secret massage phase:

This process is as follows:

Inputs: sensitive secret massage and original cover image.(any format .BMP, .PNG, etc)

Output: Stego image.

Process:

1 a) Convert the sensitive secret data into a byte array of 0s and 1s.

b) Create a checksum for the secret data's byte array format.

c) To create the codeword, combine two bytes of the determined checksum with the sensitive secret data byte array.

2 Execute the compression process using the codeword that was determined or calculated.

3 Utilizing the AES encryption technique, generates a symmetric key with a length of 128 bits at random.

b) Use the AES technique to encrypt the compressed codeword and produce the cypher data.

4 a) Use 4 bytes to compute the header. It has two bits for the length type and two bytes for the codeword.

b) Use an AES 128 bit symmetric key to secure the 4 bytes of the header.

5 a) Determine the original image's width (w) and height (h) using the original image's dimensions. Calculate or generate a secret key with a 32-bit length using the encryption algorithm, i.e. w * h.

6 a) from 0 to 4 for t

Assume the aforementioned conditions

m=0

b) array n=k

c)j pixels' coordinates are processed by the programme mapping by computing X and Y.

d) Open the original cover image and find the chosen pixel n.

e) Incorporated the encryption header data into the particular pixel of j.

f) End for with n=n+1 and k=k+1.

7 for I = 0 to l

a) Assume that the length of the original cypher text for the secret data is equal to e.

b) m=0;

c) k=array [t];

d) Calculate the j-pixel mapping process coordinates by computing X and Y.

e) Open the original cover image and find the chosen pixel j.

f) Incorporated cypher data into a particular pixel of i.

g)Let m = m + 1 and k = k + 1.

h)get the stego image

end for.

Extraction phase:

Input: OutputtedStego image.

Output: The original sensitive secret data and the original cover image .

Process**:**The reverse process of the embedding phase shown in Figure 3.

5. PERFORMANCE METRICS:

The proposed method is compared with the various existing algorithms of image steganography under spatial domain environment.

Image quality metrics:

These quality matrices are used to determine the stego image's quality in relation to the original cover image. We calculated many quality measures for the suggested technique, including PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error), Average difference (AD), Maximum difference (MD), Normalized absolute error (NAE), and Cross-correlation (CC).

The data collection at http://sipi.usc.edu/database/ contains the photos in their entirety. For the purpose of supporting the suggested method and the procedure depicted in Figures 4 to 9, we chose several colour photographs of varying sizes with various lengths of secret data. Table 1 displays the various image quality of the suggested method for photos of various sizes and embedding rates. The PSNR and MSE values for the proposed and sequential LSB methods are shown in Table 2.

Figure 4: Original Cover Image

Figure 5: Stego Image

Figure 6: Original Cover Image

Figure 7: Stego Image

Table 1: Results of the Proposed Method

Embedding Rate	Original Image	Text Message Length(bits)	PSNR	MSE	AD	MD	NAE	CC
10%	Baoo.bmp	21524	60.45	0.0031	-0.0014	6	0.0001	1
	Leena.png	21524	66.32	0.0061	-0.0013	6	0.0002	1

	Elaanie.tiff	21524	61.55	0.0045	-0.0018	6	0.0002	1
	Minii.jpg	21524	68.09	0.0023	-0.0012	6	0.0001	1
	Babo.bmp	78353	57.39	0.0024	-0.0013	6	0.0001	1
	Leena.png	78353	58.47	0.0065	-0.0011	6	0.0002	1
	Elanaie.tiff	78353	51.36	0.0034	-0.0015	6	0.0003	1
30%	Minii.jpg	78353	54.85	0.0023	-0.0016	6	0.0002	1
	Baoo.bmp	132273	53.21	0.0067	-0.0013	6	0.0002	1
	Leena.png	132273	51.23	0.0043	-0.0012	6	0.0001	1
	Elaanie.tiff	132273	56.88	0.0022	-0.0012	6	0.0002	1
50%	Minii.jpg	132273	54.98	0.0056	-0.0013	6	0.0003	1

Table 2: Comparison results of existing and proposed algorithms

Payload Size(Kbytes)	Sequential LSB Method PSNR	Propose Method PSNR	Sequential LSB Method MSE	Propose Method MSE
1	62.34	63.86	0.022	0.023
2	62.45	61.76	0.0064	0.053
4	52.34	54.56	0.0056	0.1234
8	52.67	54.32	0.2456	0.2154
16	49.87	51.45	0.456	0.345
32	46.78	49.87	0.8	0.7568
64	45.34	44.67	1.456	1.234
128	43.45	42.34	3.46	2.893
256	36.45	40.67	5.67	5.456

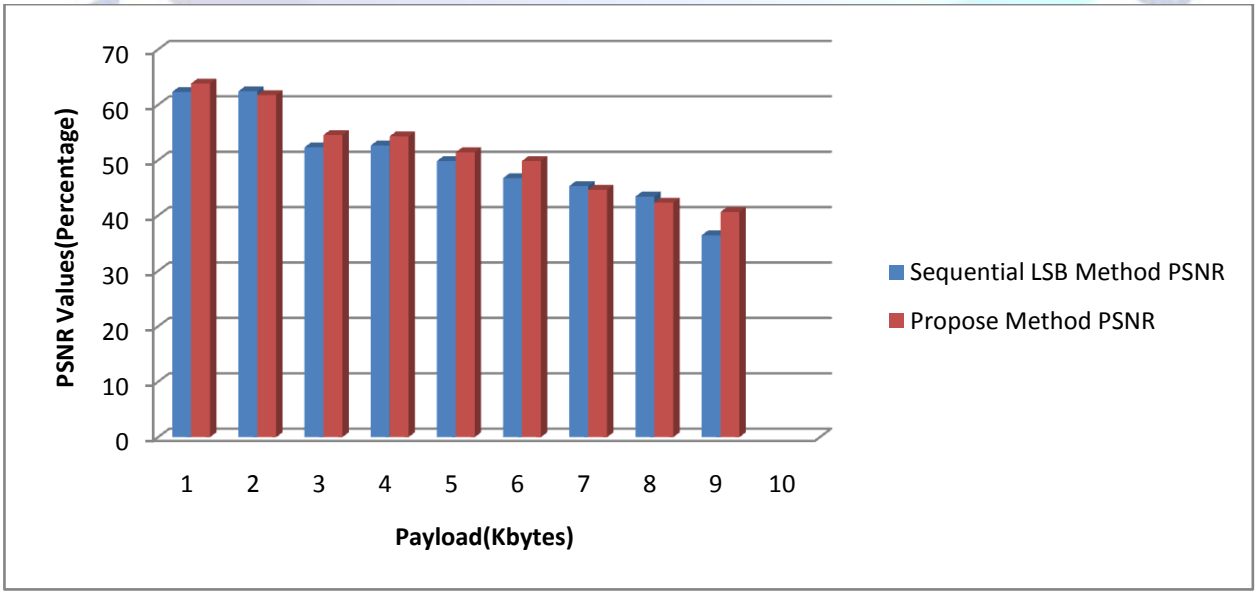

Figure 8: Comparison of Proposed Method PSNR value with Sequential LSB Technique

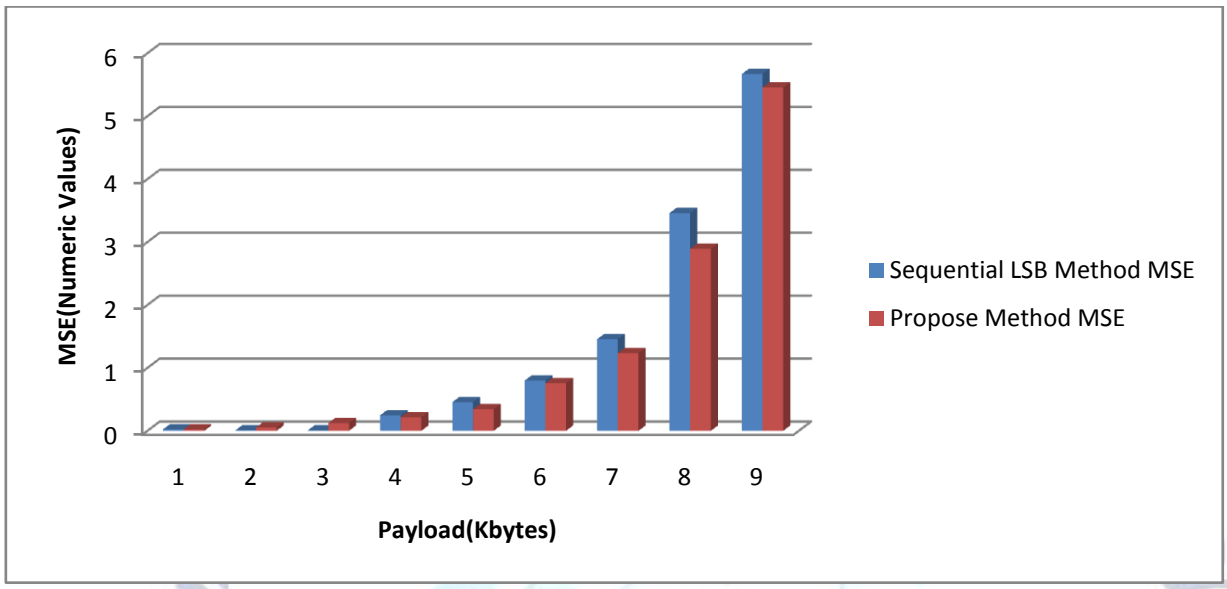

Figure 9: Comparison of Proposed Method MSE value with Sequential LSB Technique

6. CONCLUSION AND FUTURE SCOPE:

In this paper, we suggested a number of upgrades and improvements to the sequential LSB picture steganography methods already in use. The suggested approach has two levels of security. The original secret message is first encrypted using the AES technique, which also creates a cypher key. Based on the chosen pixel from the original image, the cypher key is embedded into the image at the second level. This method's improvements span a number of image quality criteria, including checksum, compression, header data, and random pixel selection. The proposed method offers better comparison outcomes when compared to different sequential LSB steganography techniques already in use. We can draw the conclusion that the suggested method satisfies a number of essential requirements for image steganography and also produces better results by comparing it to various existing methods.With an increase in PSNR values and a drop in MSE values, the suggested approach yields improved outcomes in the spatial and frequency domain. If the suggested algorithm uses more parameters and employs the principles of a Cascading feed forward network for training the chosen pixels and DCT coefficients, performance is anticipated to increase.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Chan C-K and Cheng L-M 2004 Hiding data in images by simple LSB substitution. Pattern Recognit. 37: 469–474

[2] Kukapalli V R, Rao T B and Reddy B S 2014 Image Steganograpghyby Enhanced Pixel Indicator Method Using Most Significant Bit (MSB) Compare. International Journalof Computer Trends and Technology 15(3): 97-101

[3] Dighe D and Gand Kapale N D 2013 Random InsertionUsing Data Parity Steganography Technique. Int. J. Eng. Sci.Innov Technol (IJESIT) 2(2): 364–36

[4] Dadgostar H A and Fsari F 2016 Image steganography basedon interval-valued intuitionistic fuzzy edge detection and modified LSB. Journal of Information Security and Applications(JISA). 30: 94–104

[5] Akhtar N 2016 An LSB substitution with bit inversion steganography method. In: Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics 43: 515–521

[6] Wu D-A and Tsai W-H 2003 A steganographic method for images by pixel-value differencing. Pattern Recognit. Lett.24(9–10):1613–1626.

[7] D.suneetha 2017 Data Hiding Using Fibonacci EDGE Based Steganography for Cloud Data International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 16 (2017) pp. 5565-5569

[8] Kiran 2018 A Secure Steganography Approach For Cloud Data Using Ann Along WithPrivate Key Embedding International Journal of Computer Science and Information Security (IJCSIS),Vol. 16, No. 6, June 2018

[9] D.Suneetha , 2018 Enhancement of Security for Cloud DataUsing Partition-Based Steganography,springer AISC Series

[10] Dr.R.Kian Kumar ,2019 A Novel Approach For Data Security In Cloud Environment Using Image Segmentation And Image Steganography, springer AISC Series
[11] Chandramouli, Rajarathnam, and Nasir Memon. "Analysis of LSB based image steganography techniques." Image Processing, 2015. Proceedings. 2001 International Conference on. Vol. 3. IEEE, 2001.
[12] Patil, Priyadarshini, et al. "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish." Procedia Computer Science 78 (2016): 617-624.
[13] Awwad, Yousef Bani, and Mohammad Shkoukani. "STC The Affect of Genetic Algorithms on Blowfish Symmetric Algorithm." IJCSNS 17.3 (2017): 65.
[14] Akimov, Kolesnikov. "Security implications of virtualization: A literature study." Computational Science and Engineering, 2009. CSE'09. International Conference on. Vol. 3. IEEE, 2017.
[15] Horspool. "Hide and seek: An introduction to steganography." IEEE security & privacy 99.3 (2018): 32-44.
[16] R. Chandramouli and N. Memon,"Analysis of LSB based Image Steganography", IEEE ICIP, pp. 1022-1022, Oct. 2016.
[17] R.J. Anderson, F.A.P. Petitcolas, "On The Limits of Steganography", IEEE Journal of Selected Area in Communications, pp. 474-481, May 2017.
[18] N.F. Johnson, S. Jajodia, "Stag analysis: The Investigation of Hiding Information", IEEE, pp. 113-116, 2016.
[19] H.Hastur,Mandelsteg,ftp://idea.sec.dsi.unimi.it/pub/security/crypt /code/
[20] K. Rabah, "Steganography- the Art of Hiding Data", Information Technology of Journal, 3(3), pp.245-269, 2014.
[21] N.F.Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", Computer 31, pp.26-34, 1998.
[22] F.A.P. Petitcolas, R.J. Anderson and M.G. Kuhn, "Information Hiding - A Survey", IEEE Proc., Special Issue on Protection of Multimedia Content, 87(7),pp.1062-1078, July 2015.
[23] Dr.R.Kiran kumar, 2nd International Conference on Data Engineering and Communication Technology, Advances in Intelligent Systemsand Computing 828
[24] suneetha,4 th International Conference on Information Systems Design and Intelligent Applications" held during 19th-21st July, 2018
[25] Chandramouli, Rajarathnam, and Nasir Memon. "Analysis of LSB based image steganography techniques." Image Processing, 2001. Proceedings. 2001 International Conference on. Vol. 3. IEEE, 2017.
[26] Patil, Priyadarshini, et al. "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish." Procedia Computer Science 78 (2016): 617-624.
[27] Awwad, Yousef Bani, and Mohammad Shkoukani. "STC The Affect of Genetic Algorithms on Blowfish Symmetric Algorithm." IJCSNS 17.3 (2017): 65.