

Review on Steganography Techniques

Mohit Goel

School of Electronics and Communication
Lovely Professional University, Punjab
Mohit.16907@lpu.co.in

Abstract

With increase in use of internet, user wants to access the data easily and securely at any spot of time. So, user start saving and sharing the important information on cloud. Hence, the security of data on cloud computing become a major issue of concern. Steganography is used as a standard practice for both cloud service providers and cloud users as a tool against unauthorized surveillance. Steganography refers to guarding the information by concealing it in some other media such that only the owner has the ability to safely recover the information. The purpose of this paper is to give an overview of different techniques of steganography used in cloud computing and compare them on the parameters like, technique selection, carrier formats, payload capacity.

Keywords: *steganography; encryption; data hiding.*

I. INTRODUCTION

In the last few years, a cloud computing has become a propensity in information technology as it leads to significant amount of reductions in costs and help to expand the business to its users and providers [1]. Cloud computing is defined by the National Institute of Standards and Technology (NIST) as : "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". Even though cloud computing applications are only at the development phase, significant barriers that are related with adopting cloud computing, such as security issues, compliance and legal matters [8,9]. Two techniques are developed to protect the information: steganography and cryptography. Steganography is often confused with cryptography although the two are completely different terms. Cryptography manages privacy, while steganography manages secrecy [7]. Steganography is the science of securing information among a carrier object such that solely the sender and receiver have the power to recognize and observe the hidden information and safely transfer it through the means of communications. Steganography is a combination of two words Stegano + Graptos. Stegano means "covered" and graptos means "writing" which exactly means "covered writing" [10]. While, the study of means of converting information from its normal form into a coded format is called cryptography.

II. LITERATURE SURVEY

A. Spatial Domain

R. Shanthakumari et.al have proposed a technique for video steganography using LSB matching revisited algorithm [11]. In this technique the LSB matching revisited algorithm selects the region (region in a frame) of embedding according to the size of the message to be embedded and the distance between two consecutive pixels in the cover image. Now the secret key is calculated using the Diffie Hellman algorithm which is a method that allows sender and receiver who have no prior knowledge of each other to jointly generate a shared secret key over a secured communication channel and then the cover image is divided into non-overlapping blocks and each block is rotated by a factor, determined by the secret key and this block is then rearranged as a row vector using raster scanning and this vector is divided into non-overlapping units with every two consecutive pixels which can be used to generate a pseudo random number (which can be even or odd). Here there are two advantages of rotating the image block of which one is, it prevents the intruder from finding out the correct embedded bits by increasing the security as the rotating factor a being a secret key and the second advantage is that both the vertical and horizontal edges within the cover image can be used for embedding the secret message. Therefore, in this security is improved and as steganography here is implemented on video, there is enough space for data to be hidden.

S.K.Muttoo et.al have proposed a technique for multilayered secure, robust and high capacity image steganographic algorithm [12]. In this technique the data to be hidden is first encoded/compressed using T-codes and then this encoded/compressed data is encrypted using improved Advanced Encryption Standard (AES) encryption. Now this encrypted data is hidden in the high frequency components which are obtained by the performing level-1 Double density dual tree discrete wavelet transform (DD DT DWT) on the cover image. In this there is three layer security one at each layer i.e. at encoding/compression, encryption and embedding, thus this proposed method provides better capacity with the use of DD DT DWT instead of DWT and is highly secured due to the 3 layer security provided and also steganography implemented in frequency

domain is considered to be more secure than in spatial domain.

Dr. V. Vijayalakshmi et.al have proposed a technique for a modulo based LSB steganography that can effectively resist steganalysis of image based on histogram analysis and statistical analysis [15]. In this method a pseudo random number is generated which is used to select the number of pixels from the cover image to hide the data and combines the samples of the LSB bits of the cover image by addition modulo and forms a value which is then to be compared with the LSB of message data. If there two values of cover image LSB bit value by addition modulo and the message data are equal, there is no change to be made and if the values are not equal the difference of the two values is added to the sample. The proposed method is for both color and black and white images. As this method is proposed to effectively resist the steganalysis of image based on histogram and statistical analysis, security has been enhanced but not the capacity since it is working on pseudo random number generation.

Nadeem Akhtar et.al have proposed a technique for an improved inverted LSB image steganography in which the concept of bit inversion technique is been used to improve the quality of the stego image [16]. In this method the LSB's of some of the pixels of the cover image are inverted if they occur with a particular pattern, by this way less number of pixels are changed thereby improving the quality of the stego image. But for the extraction of the message from the stego image the bit patterns for which the LSB's have been inverted needed to be stored within the stego image itself. This could be taking more space from the cover image for hiding as it is important to save pixels for storing the bit patterns also which is not capacity efficient. Therefore, in this image neither capacity nor security is enhanced but only the quality of the stego image is been improved.

P Sandeep Reddy et.al have proposed a technique for hiding image in video in which the image steganography algorithm used gray codes and secret keys for hiding the data securely [17]. The algorithm takes any input image of any format like .jpg, .png, .tiff, .bmp etc. and this input image is converted to bmp format because of the reason bmp file format uses lossless compression so that the compression of .bmp image does not lose any information. As said, in this algorithm data first encrypted and then hidden in the cover image or a frame of the video. The encryption technique here used is by performing SN function which uses the gray codes and the symmetric keys for encrypting the data. The main advantage of SN function is that it can encrypt plain text and also decrypt the cipher text with small changes.

Sunny Dagar have proposed a technique for highly randomized image steganography using secret keys in which two different keys are used for hiding process randomly [20]. This approach uses the values pixels from red, green and blue planes for calculations of some values and with the help of these values the message data bits are hidden in the cover image at random positions of the pixels. The process of calculation of values is as, in this method two keys are used for embedding, the information securely. So first the MSB bit of first red pixel is taken and the first bit from first key is taken and xor operation is performed between them and according to the resultant decision is made whether to hide the secret message data in green plane or blue plane and using the second key the position of where to hide in the green or blue plane is known. Therefore, this approach is efficient in both capacity and as well as security since the randomized hiding improves the security level of embedding.

M. Radhika et.al have Mani proposed a technique for an innovative approach for pattern-based image steganography in which the message data is hidden in the cover image according to some pattern [21]. The pattern with this method goes like, first the cover image is divided into non-overlapping blocks of size 25x25 and within each 25x25 block the block is further divided into 5x5 non-overlapping sub blocks. Now the 5x5 blocks within the 25x25 block is selected by a pattern letter 'Z' and the LSB bit of the pixel is replaced with the LSB bit of the message data according to a pattern 'α'. Although this method did not tell about the flexibility of changing the patterns but it improved by changing the pattern and the two patterns can be used as two keys which also improves security but as far as this method is concerned it has enhanced security a little but it is not robust since adding of any extra noise leads to complete destroy of the message data.

Sara sajasi et.al have proposed a technique for a high-quality image steganography scheme based on fuzzy inference system [23]. In this method fuzzy inference system (FIS) is used to determine the complexity of each block and get the payload information for the block to hide the data. In this method the cover image is divided into non-overlapping blocks of 3x3 size and each block is processed with Fuzzy inference system with some features (edge sensitivity, brightness, texture feature etc.) as input and according to these features it gives the degree of membership value as output for each block which is the parameter for deciding the payload information for embedding number of bits into the block with various conditions. The disadvantage of this method could be it requires extra 2 bits per pixel to store the type of FIS it is. So this method is concentrated only

on increasing the quality of the image and embedding capacity.

S. M. Masud Karim et.al have proposed a technique for a new approach for LSB based image steganography using secret key [24]. This approach is a new approach to improve the existing LSB technique. In this method a secret key is used which is used along with the red plane to decide in which plane either green plane or blue plane to hide the message data. So in this method a secret key is converted into binary form array and the message data is also converted into a binary array. Now the first bit of secret key and the LSB bit of the first pixel of the red plane is taken and xor operation is performed, if the resultant is 1 then the message data bit is stored in the green plane and if the resultant is 0 the message data is stored in the blue plane. So, this method enhances security by adding the secret key for selecting plane for hiding the data and the embedding capacity of this algorithm is also good.

Geetha C.R. et.al have proposed a technique for variable load image steganography using multiple edge detection and minimum error replacement [28]. The hiding process in this proposed technique is done on the edge pixels of an image since the changes made in the edge pixels are insensitive to the human eye. In this method edge detection technique is applied cover image and the gradient of the image is determined, now a threshold value is selected and compared with the pixel gradients and if the gradient value is lesser than the threshold value, it is not an edge pixel and the rest are edge pixels. This method is repeated multiple times i.e. the edge detected image is again subjected to the edge detection technique which doubles the number of edge pixels in an image. More number of edge pixels more capacity for hiding. Now using variable embedding ratio the number of bits of secret message data to be hidden in the edge pixels and non-edge pixels is decided and the data is hidden according to the ratio and the minimum error is calculated between the newly formed stego image and the cover image. If the error is more than the previous value, the bit is changed to its original value and if the error is less the bit is unchanged. So, by this method capacity is increased by multiple edge detections and security is also increased by the variable embedding ratio and also the quality of the image is increased by minimum error replacement.

Ankit Chaudhary et.al have proposed a technique for hash-based approach for secure keyless image steganography in lossless RGB images, which is based on the pixel indicator technique [5]. In this approach the cover image is the RGB image and the three planes red, green and blue are used to hide the message bits. The sequence in which planes has to

hide the message bits is determined by the value MSB's of the red, green and blue pixels and also it is taken care that the message bits are not embedded in the top of the image rather the message bits are hidden over the entire image. This is achieved by calculating a key value with the help of image size and the message length so that the message bits are embedded in the pixels after the key value difference. Therefore, this method is for hiding the text messages in an image and this method improves the quality of the image by using only 3 bits per pixel and increases security level by hashing and also the embedding capacity is increased by using all the three planes for hiding.

B. Transformational Domain

Mohammad Reza Dastjani Farahani et.al have proposed a technique for a DWT Based Perfect Secure and High Capacity Image Steganography [13]. This method is used for pictorial messages in cover images. In this a same level DWT is applied to both the message data and the cover image data, thereby generating four frequency components i.e. CCA (low frequency components), CCH (horizontal), CCV (vertical) and CCD (diagonal) of the transformed cover image and similarly for the message data too i.e. MCA, MCH, MCV, MCD. Now the CCA and MCA coefficients are divided into 4x4 blocks and the most similar blocks of the CCA and MCA are found using root mean square error (RMSE) pattern matching distance criterion and these similar block numbers are saved as keys. According to this there is no replacement or combination between the message DWT coefficients and the cover image DWT coefficients, therefore the cover image will remain unchanged. Hence this method is called as perfect square method. This method is high capacity image steganography method and also security is enhanced.

Sudhir Keshari et.al have proposed a technique for Weighted Fractional Fourier Transform based Image Steganography in which the secret image to be sent is hidden in intermediate domain between spatial and frequency of the cover image by weighted fractional Fourier transform (WFRFT) [14]. In this the cover image is divided into 2x2 blocks and WFRFT with a transform order a is performed on each block. The intermediate domain consists of both real and imaginary components. Concentrating only on the real part, convert into binary form on considering absolute real values. Now the first pixel of the message image is selected and converted to binary form and then its two LSB bits are taken and are inserted into the two LSB bit positions of each pixels of 2x2 window. In this method the key is the transform order a which the intruder does not know with what transform order WFRFT is performed and

this is also an advantage over conventional Fourier transform. So, in the method only security is enhanced.

K B Shiva Kumar et.al have proposed a method for bit length replacement steganography based on DCT coefficients [18]. In this method the data hiding process is done in the transformational domain which is by performing 2D-DCT on the cover image, but before applying 2D-DCT on the complete image the cover image is firstly divided into 8x8 non-overlapping blocks and then 2D-DCT is performed on each block. By doing in this way the computational time for embedding the data and security to payload increases. After performing 2D-DCT and getting the coefficients, a coherent bit length is calculated which determines the number of LSB bits of the each DCT coefficients that can be used for hiding the MSB bits of data.

Reba Mostafa et.al have proposed a technique for Hybrid curvelet transform and least significant bit for image steganography in which first curvelet denoising is applied on the image as a pre-processing step to remove the noise from the cover image [19]. The cover image is then transformed into the frequency domain using curvelet transform. The curvelet transform is a multiscale geometric analysis with which the image features can be shown both at each scale and different directions and also curvelet transform is been chosen because this transform can handle the curve discontinuities in an image for better robustness and quality of the image. Now cover image is divided into blocks of 8x8 size and the message data to be hidden in the cover image is embedded in the curvelet coefficients without making any changes that can be noticeable in the cover image. Therefore, in this method only quality is been improved.

Neda Raftari et.al have proposed a technique for digital image steganography based on assignment algorithm and combination of DCT-IWT in which the secret message is embedded in the frequency domain with high matching quality with the help of Munkres' assignment algorithm [27]. In this method the firstly DCT is applied on the secret image and apply 2D haar integer wavelet transform on the cover image and the DCT coefficients of the secret image and find the four sub bands (CCA, CCD, CCV, CCH and ICA, ICV, ICH, ICD). Now each of the CCA, ICA and ICH are divided into non-overlapping blocks of size 2x2 and for each block in CCA the best matched block in ICA is found using the root mean square error technique. This is the first secret key which is the location of the matched block in ICA. After this the best matched block is searched in the ICH sub band by Munkres' assignment algorithm and replace these blocks with the matched blocks

which are acquired by the root mean square method. The second key here is the block location that is matched with the ICH block, after this apply inverse haar integer wavelet to get the stego-image. So this method is towards the improvement of the security by two keys but the embedding capacity is not improved.

Prajanto Wahyu Adi et.al have proposed a technique for a high-quality image steganography on integer haar wavelet transform using modulus function [4]. In this method before the embedding of the message a threshold value is decided which will determine the hiding capacity and also this threshold value prevents the reconstructed image while extracting fall out of pixel intensity of range 0 to 255. A random 8-bit unsigned key is used to scramble the message or encrypt the message. Now perform IHWT – integer haar wavelet transform on the cover image and all the four sub-bands are found. Then the remainder of two adjacent pixels is found by the modulus operation with 2^T and embed T-bits of the message into the image by adjusting the adjacent pixels according to the condition defined. After the embedding is done perform inverse integer haar wavelet transform to obtain the stego image. Therefore, by this proposed method the quality of the image is increased since the method tries to make smaller adjustment values to the coefficients which improves the imperceptibility of the image.

C. Multi-layer steganography

Ramadhan J. Mstafa et.al have proposed a technique for video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes method in which a frame is selected from the video and for hiding the message data, a region of interest is selected from the selected frame like facial regions etc [22] and the LSB's of the ROI is replaced but the pre-processed message data bits. The message data bits are pre-processed using hamming codes (15, 11) which denotes data word is of 11 bits and after adding of 4 redundancy bits for error detection and correction purpose the data word now becomes 15 bit length which is called as code word, this code word is sent to the receiver and the receiver can verify whether the message he received after the extraction of message from the cover frame by checking the syndrome bits by forming a matrix. If the extracted message is error free the syndrome bits must be all zero but if in case any bit is error the syndrome value changes and the use can know by that. So, in this method security is improved by using the hamming codes and also by selecting the region of interest, and as steganography is performed on video there is not capacity embedding factor there is enough space for the data to be hidden.

Kamaldeep Joshi et.al have proposed a technique for a new LSB-S image steganography method blend with cryptography for secret communication [25]. LSB-S means LSB with shifting. This method used the combination of cryptography and steganography for embedding the message data as two-level security. In this method a grayscale cover image is taken and converted into binary format and the message data is encrypted by using Vernam cipher and then converted into binary form. Now extract four LBS's of each pixel from the cover image and then left shift them by 1 bit and now take the LSB of the left shifted data and perform XOR operation with the message data first bit and the resultant is the bit value at the LSB's position of the cover image. So, this method has improved security by two level security using cryptography and steganography and also the embedding capacity of this method is 100% as all the pixels can be used for hiding.

RigDas et.al have proposed a technique of novel steganography method for image based on Huffman coding [26]. In this method Huffman encoding is performed on the message data before embedding and each bit of the Huffman code of the message data is stored in the cover image by replacing it with the LSB bit values of the pixels of the cover image. In this method after obtaining the Huffman table for the message data or the secret message, the Huffman encoding is performed on the message data and the Huffman encoded bit stream is calculated. The size of the Huffman encoded bit stream should also be calculated. Now there arises a problem that if this Huffman size is stored in the cover image so as to know till where data is been encoded in the cover image, what is or what would be the size of the Huffman encoded bit stream. This problem is solved by the four-tier storage of the size by which the size of the Huffman encoded bit stream is reduced to two bits after the four-tier storage. Now store the Huffman size in the block of size 8x8 of cover image at its LSB positions and also store the Huffman encoded bit stream in the pixels excluding the first where size is stored and also store the Huffman table. This method improves the security and as well as the quality of the stego-image.

III. RESULT AND CONCLUSION

Throughout this paper a brief introduction to steganography and different steganography techniques are reviewed, by which a basic ideology is provided on steganography. In spatial domain although there is a high payload or high capacity to embed the data this method is more prone to attacks as it has weak resistance while the transformational domain techniques are less prone to attacks and other transforms on data especially when the data hidden is small but are of less payload or low capacity for

embedding the data also these methods have less distortion of cover image and is more secure than spatial domain techniques. Steganography is not only for secure communication of data but can also be used for a secure storage system such as storing any valuable information in the database, e.g. e-commerce companies like flipkart, amazon and many more who store many customers valuable data in their databases can use steganography for hiding those information safely from intruders.

References:

- [1] Palak Patel and Yask Patel, "Secure and authentic DCT image steganography through DWT- SVD based digital watermarking with RSA encryption", IEEE Fifth International Conference on Communication Systems and Network Technologies 2015.
- [2] Barnali Gupta Banik and Samir Kumar Bandyopadhyay, "Implementation of Image Steganography Algorithm using scrambled Image and Quantization coefficient modification in DCT", IEEE Conference on Research in Computational Intelligence and Communication Networks 2015.
- [3] Prajanto Wahyu Adi, Farah Zakiyah Rahmanti and Nur Azman Abu, "High Quality Image Steganography on Integer Haar Wavelet Transform using Modulus Function", IEEE 2015 International Conference on Science in Information Technology (ICSITech).
- [4] Ankit Chaudhary and JaJdeep Vasavada, "A Hash Based Approach for Secure Keyless Image Steganography in Lossless RGB Images", IEEE First International Workshop on Cyber Crime 2012.
- [5] Prabakaran. G and Bhavani R, "A modified secure digital image steganography based on Discrete Wavelet Transform", IEEE International conference on Computing, Electronics and Electrical Technologies 2012.
- [6] Dr. Mahesh Kumar and Munesh Yadav, "Image Steganography using Frequency Domain", International journal of Scientific and technology research, Volume 3, Issue 9, PP: 226 - 230, SEPT 2014.
- [7] Shahana T, "A Secure DCT Image Steganography based on Public-Key Cryptography", International Journal of Computer Trends and Technology, Volume 4, Issue 7, PP: 2039 - 2043, JULY 2013.
- [8] Pritam Kumari, Chetna Kumar, Preeyanshi and Jaya Bhushan, "Data Security Using Image Steganography and Weighting its Techniques", international journal of scientific & technology research volume 2, issue 11, PP: 238 - 241, Nov 2013
- [9] Dr. Sudeep D. Thepade and Mrs. Smita S. Chavan, "Vigorous Image Steganography with Transforms, Wavelet Transforms and Hybrid Wavelet Transforms", IEEE India Conference, 11 - 13 DEC 2014.
- [10] Er Prajna Vasudev and Er Kumar Saurabh, "Video Steganography using 32*32 Vector quantization of DCT", International Journal of Software and Hardware Research in Engineering, Volume 1, Issue 3, PP: 40 - 43, NOV 2013.
- [11] R.ShanthaKumari and Dr.S. Malliga, "Video steganography using LSB matching revisited algorithm", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-

0661, p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. IV (Nov – Dec. 2014), PP: 01-06.

[12] Sunil Muttoo and Sushil Azad, "A multilayered secure, robust and high capacity image steganography algorithm", World of Computer Science and Information Technology Journal (WCSIT), ISSN: 2221-0741, Vol. 1, No. 6, PP: 239-246, 2011.

[13] Mohammad Reza Dastjani Farahani and Ali Pourmohammad, "A DWT Based Perfect Secure and High Capacity Image Steganography Method", IEEE International Conference on Parallel and Distributed Computing, Applications and Technologies 2013.

[14] Sudhir Keshari and Shri Gopal Modani, "Weighted Fractional Fourier Transform based Image Steganography", IEEE International Conference on Recent Trends in Information Systems 2011.

[15] Dr. V. Vijayalakshmi, Dr. G. Zayaraz, and V. Nagaraj, "A Modulo Based LSB Steganography Method", IEEE international conference on "control, automation, communication and energy conservation" -2009, 4th-6th June 2009.

[16] Nadeem Akhtar, Shahbaaz Khan, and Pragati Johri, "An improved inverted LSB image steganography", IEEE, 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT).

[17] P Sandeep Reddy and Kalpana Reddy, "Hiding image in video", International Journal of Research Sciences and Advanced Engineering [IJRSAE] TM Volume 2, Issue 8, PP: 87 - 91, OCT - DEC 2014.

[18] K B Shiva Kumar, K B Raja, R K Chhotaray, and Sabyasachi Pattanaik, "Bit length replacement steganography based on DCT coefficients", International Journal of Engineering Science and Technology, ISSN: 0975-5462, Vol. 2(8), 2010, PP: 3561-3570, ResearchGate.

[19] Reba Mostafa, Ahmed Fouad Ali, and Ghada EI Taweal, "Hybrid curvelet transform and least significant bit for image steganography", 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS'15).

[20] Sunny Dagar, "Highly randomized image steganography using secret keys", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014.

[21] M. Radhika Mani, V. Lalithya, and P.Swetha Rekha, "An innovative approach for pattern based image steganography", 2015 IEEE.

[22] Ramadhan J. Mstafa and Khaled M. Elleithy, "A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes, Springer Science+Business Media New York 2015.

[23] Sara sajasi and Amir Masoud Eftekhari Moghadam, "A high quality image steganography scheme based on fuzzy inference system", 2013 IEEE 13th Iranian Conference on Fuzzy Systems (IFSC).

[24] Manishaben Jaiswal, "COMPUTER VIRUSES: PRINCIPLES OF EXERTION, OCCURRENCE AND AWARENESS ", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.5, Issue 4, pp.648-651, December 2017, <http://doi.org/10.1729/Journal.23273> Available at http://www.ijcrt.org/viewfull.php?&p_id=IJCRT1133396

[25] Manishaben Jaiswal "Big Data concept and imposts in business" International Journal of Advanced and Innovative Research (IJAIR) ISSN: 2278-7844, volume-7, Issue- 4, April 2018 available at: http://ijairjournal.in/Ijair_T18.pdf

[26] Manishaben Jaiswal " SOFTWARE QUALITY TESTING " International Journal of Informative & Futuristic Research (IJIFR) , ISSN: 2347-1697 , Volume 6, issue -2 , pp. 114-119 ,October-2018 Available at: <http://ijifr.com/pdfsave/23-12-2019214IJIFR-V6-E2-23%20%20OCTOBER%202018%20a2%20files%20mergeda.pdf>

[27] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A new approach for LSB based image steganography using secret key", IEEE Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 201 I) 22-24 December, 2011.

[28] Kamaldeep Joshi and Rajkumar Yadav, "A new LSB-S image steganography method blend with cryptography for secret communication", IEEE 2015 Third International Conference on Image Infonation Processing.

[29] RigDas and Themrichon Tuithung, "A Novel Steganography Method for Image Based on Huffman Encoding", 2012 IEEE.

[30] Neda Raftari and Amir Masoud Eftekhari Moghadam, "Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT", IEEE 2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks.

[31] Geetha C.R., Basavaraju.S and Dr.C. Puttamadappa, "Variable load image steganography using multiple edge detection and minimum error replacement method, IEEE Proceedings of 2013 IEEE Conference on Information and Communication Technologies (ICT 2013).